

# Department of Defense Full Spectrum Integrated Vulnerability Assessment Program

## Critical Infrastructure Protection Capability Area Standards



15 January 2004

For Official Use Only



**The Defense Program Office for  
Mission Assurance**

---

**Department of Defense  
Full Spectrum Integrated Vulnerability Assessment Program**

**Draft  
Critical Infrastructure Protection Capability Area Standards**

---

**January 15, 2004**

**Naval Surface Warfare Center, Dahlgren Division  
17320 Dahlgren Road  
Dahlgren, VA 22448-5100**

For Official Use Only

**For Official Use Only  
Draft CIP FSVA Standards**

**CONTENTS**

<b><u>Section</u></b>	<b><u>Page</u></b>
1.0 PURPOSE OF FSIVA STANDARDS .....	1
2.0 OBJECTIVE OF FSIVA STANDARDS .....	1
3.0 SCOPE.....	1
4.0 DEVELOPMENT OF THE FSIVA STANDARDS .....	1
5.0 FSIVA STANDARDS FORMAT .....	2
6.0 USE OF THE FSIVA STANDARDS.....	3
7.0 UNDERSTANDING THE EVOLVING CIP ENVIRONMENT.....	4
ACRONYM LIST.....	273

**Standards**

PHYSICAL SECURITY .....	6
Outer Perimeter Security .....	6
Parking.....	6
Standoff/Setback.....	8
Proximity to High-Value Targets .....	11
Outer/Inner Perimeter, Security .....	13
Monitoring .....	13
Outer Perimeter Security .....	15
Physical Barriers.....	15
Perimeter Security.....	19
Exterior Security Lighting.....	19
Security Force Operations (SFO).....	21
Access Control.....	23
Entrances and Exits.....	28
Receiving and Shipping .....	30
Construction and Design .....	33

**For Official Use Only  
Draft CIP FSVA Standards**

**CONTENTS (CONTINUED)**

<u>Standards</u>	<u>Page</u>
Interior Security.....	35
Utilities.....	35
Lock/Key Control.....	39
Compartment Area Access.....	42
Training.....	46
INFORMATION SECURITY.....	49
Physical Access Controls.....	49
Rules of Behavior.....	49
Auditing.....	55
Data Storage, Control, and Access.....	57
Records Management.....	57
Backup On-site.....	60
Alternate Site.....	62
INFORMATION SECURITY.....	63
NETWORK SYSTEMS.....	63
Maintenance.....	63
Network Systems.....	65
Intrusion Detection System and Network Boundary Control.....	65
Internal Network Security.....	68
Malicious Code.....	69
Environmental Controls.....	71
Training.....	73
End-User and System Staff Training.....	73
PERSONNEL/INDUSTRIAL SECURITY.....	75
Clearances.....	75
Contractors and Service Providers.....	75
Federal Employees.....	77
Credentials.....	79
Training.....	81
Document Control and Accountability.....	83
Classification and Marking.....	83
Safeguarding Procedures.....	85
SAFETY.....	88
Safety in the Operating Environment.....	88

**For Official Use Only**  
**Draft CIP FSVA Standards**

**CONTENTS (CONTINUED)**

<u>Standards</u>	<u>Page</u>
Facility Life Safety .....	88
Equipment/Operator Safety .....	90
Ammunitions and Explosives Safety .....	92
Fire Prevention .....	95
Training .....	96
PLANS .....	97
Training .....	97
Emergency Response Planning - Critical Asset Personnel.....	97
Emergency Preparedness.....	99
Emergency Response Planning - First Responders .....	99
Emergency Response Planning - Supporting Local, State, and Federal Response Agencies.....	101
Emergency Response Planning.....	103
Continuity of Operations (COOP).....	103
Intelligence Sharing .....	105
Coordination With External Agencies .....	105
Internal Dissemination of Security Intelligence .....	107
OPERATIONS SECURITY (OPSEC) .....	109
Information Management.....	109
Training .....	113
SECURITY OF NUCLEAR CRITICAL ASSETS .....	115
Personnel Reliability .....	115
Personnel Reliability Program (PRP) .....	115
Nuclear Facility Security .....	118
Nuclear Weapon System Safety .....	122
Storage Design Criteria .....	124
Security Force Operations (SFO).....	129
Training .....	132
SECURITY OF CHEMICAL CRITICAL ASSETS .....	135
Personnel Reliability .....	135
Personnel Reliability Program (PRP) .....	135
Facility Security .....	138
Safety and Occupational Health .....	141
Storage Design Criteria .....	144

**For Official Use Only**  
**Draft CIP FSVA Standards**

**CONTENTS (CONTINUED)**

<u>Standards</u>	<u>Page</u>
Material Control/Handling Procedures.....	147
Security Force Operations (SFO).....	149
Training.....	152
<b>SECURITY OF BIOLOGICAL CRITICAL ASSETS.....</b>	<b>154</b>
Personnel Reliability.....	154
Personnel Reliability Program (PRP).....	154
Biological Facility Security.....	156
Safety Protocols.....	165
Storage Design Criteria.....	167
Material Control and Handling Procedures.....	170
Security Force Operations (SFO).....	173
Training.....	176
<b>SUPPORTING INFRASTRUCTURE NETWORKS.....</b>	<b>178</b>
Energy.....	178
Natural Gas.....	178
Petroleum, Oil, and Lubricants (POL).....	181
Electric Power.....	185
Transportation Networks.....	190
Railroad.....	190
Highway.....	194
Air.....	198
Seaports (Seaports and Prepositioning).....	202
Communications.....	206
Electronic Voice and Data Communications.....	206
Water Systems.....	208
Potable, Industrial, and Fire Fighting Water.....	208
Water.....	212
Wastewater.....	212
Supporting Utilities.....	216
Heating, Ventilation, and Air Conditioning (hvac).....	216
<b>AVAILABILITY OF SUPPORTING MATERIEL AND SERVICES.....</b>	<b>219</b>
Source of Production.....	219
Production Capability.....	219
Commercial Relationships.....	222
Ownship of Sources of Supply.....	222

**For Official Use Only**  
**Draft CIP FSVA Standards**

**CONTENTS (CONTINUED)**

<u>Standards</u>	<u>Page</u>	
Contractor Support of Systems .....	224	
Trading Partner Security .....	226	
Transit .....	227	
Transport Capability .....	227	
Conveyance and Procedural Security .....	230	
 WEAPONS OF MASS DESTRUCTION (WMD) VULNERABILITY		
ASSESSMENT AND ANALYSIS .....	233	
WMD Response .....	233	
N/ AWMD Response - Initial Actions/Recovery/Continuity of Operations (COOP) .....	233	
WMD Avoidance and Response .....	236	
WMD Response - WMD Avoidance .....	236	
 WEAPONS OF MASS DESTRUCTION (WMD) .....		240
Chemical, Biological, and Radiological .....	240	
WMD Preparedness .....	240	
WMD Preparedness - Plans and Training .....	241	
 EMERGENCY OPERATIONS .....		245
Damage Control and Recovery .....	245	
Continuity of Operations (COOP) .....	245	
Damage Control and Recovery .....	249	
Emergency Preparedness .....	251	
Emergency Preparedness - Planning .....	251	
Emergency Response .....	256	
Emergency Response - External .....	256	
Emergency Response - Internal .....	259	
Emergency Preparedness .....	262	
Emergency Preparedness - Mitigation .....	262	
Emergency Preparedness - Threat and Hazard Identification .....	265	
 STRUCTURAL RESPONSE .....		268
Critical Equipment/Component Damage .....	268	
Protection .....	268	
New Construction or Renovation .....	270	
Protective Design .....	270	

**For Official Use Only  
Draft CIP FSVA Standards**

**CONTENTS (CONTINUED)**

<u>Standards</u>	<u>Page</u>
THREAT .....	272
Electromagnetic Threats.....	272
RF Weapons, EMP, Grounding, Bonding, Lightning Protection.....	272

# **For Official Use Only**

## **Draft CIP FSVA Standards**

### **1.0 PURPOSE OF FSIVA STANDARDS**

The purpose of the Full Spectrum Integrated Vulnerability Assessment (FSIVA) Critical Infrastructure Protection (CIP) capability area standards, as set forth by the Defense Program Office for Mission Assurance (DPO-MA), is two-fold. First, this document prescribes the areas that will be assessed during the conduct of FSIVAs within the CIP capability area on Department of Defense (DoD)-designated critical infrastructure assets. Second, the document identifies and defines a comprehensive, uniform set of assessment standards to be used to identify vulnerabilities associated with those designated critical assets.

### **2.0 OBJECTIVE OF FSIVA STANDARDS**

The overall objective of the CIP capability area standards is to provide trained assessors with critical asset assessment requirements that will support the identification and evaluation of specific vulnerabilities of DoD-designated critical assets. Specifically, the CIP capability area standards will:

- a. Establish a baseline set of standards for the assessment of vulnerabilities of DoD-identified and -designated critical assets that can be used in conjunction with a threat analysis to identify potential vulnerabilities associated with designated critical assets and their supporting infrastructure.
- b. Provide a pathway for identifying additional and/or unknown supporting infrastructure dependencies that may threaten and/or impact the availability of DoD's designated critical assets.
- c. Ensure that a vulnerability assessment of DoD's critical assets is sufficiently comprehensive and appropriately detailed to identify all critical asset vulnerabilities.

### **3.0 SCOPE**

This compendium of standards is applicable to all DoD critical assets, including non-DoD federally-owned or leased critical assets and commercial critical assets that support the DoD mission.

### **4.0 DEVELOPMENT OF THE FSIVA STANDARDS**

## **For Official Use Only**

### **Draft CIP FSVA Standards**

As an initial step in developing the standards, existing vulnerability assessment activities and their methodologies both internal and external to the DoD were examined in depth. The intent of this examination was to identify the best available standards, guidelines, and best practices from existing assessment activities and determine the applicability of the standards, guidelines, and best practices to the assessment of DoD critical assets. Once the available information was identified and its applicability to an assessment of critical assets was determined, the information was used as the foundation for the development of the CIP capability area standards. This foundation established a basis for the CIP capability area standards, rooted in already accepted vulnerability assessment performance standards and guidelines. The adapted CIP capability standards were then tailored, as required, to ensure their applicability to the broadest possible range of potential critical assets. For those assessment areas where no security standards or guidelines were available, original assessment standards were derived from lessons learned from vulnerability assessments performed on assets belonging to various government departments/agencies and private industry.

#### **5.0 FSIVA CIP CAPABILITY AREA STANDARDS FORMAT**

Given the large degree of variance in what can be designated as a critical asset, the CIP capability area standards must be of sufficient breadth and depth to provide for a comprehensive assessment of any critical asset's vulnerabilities. To meet this need, the CIP capability area standards are written using a format designed to articulate the **what, why, and how** of critical asset assessment standards within the context of the CIP environment. This format provides information in a "general-to-specific" manner, intended to ensure the user clearly understands the context as well as the detailed criteria for each assessment area.

The following information, listed below, is an explanation of the standards format used in this document.

- a. AREA OF CONCERN: This section identifies the broad areas to be addressed in an assessment of designated critical assets. Areas of concern to be addressed in FSIVAs are:
  1. Physical Security
  2. Information Security
  3. Personnel/Industrial Security
  4. Safety
  5. Plans
  6. Operations Security

## For Official Use Only Draft CIP FSVA Standards

7. Security of Nuclear Critical Assets
  8. Security of Chemical Critical Assets
  9. Security of Biological Critical Assets
  10. Supporting Infrastructure
  11. Availability of Supporting Materiel and Services
  12. DTRA-Recommended Weapons of Mass Destruction
  13. DTRA-Recommended Emergency Operations
  14. DTRA-Recommended Structural Response
  15. DTRA-Recommended Threat
- b. TOPIC and SUBTOPIC: These sections identify the lower-level topics and subtopics that are associated with each of the broad areas of concern.
- c. EXPLANATION: This section briefly describes what each topic or subtopic covers.
- d. INTENT: This section explains the objective of an assessment of the identified topic or subtopic area. This is to ensure users of this document understand the larger context of the assessment.
- e. DESCRIPTION: This section explains to a greater degree of specificity what will be included in an assessment of the subtopic area.
- f. CRITERIA: This section contains specific DoD, Service, Agency, and Defense Industrial Base references, standards, and suggested recommendations that may apply to the Area of Concern, topic, and/or subtopic. The actual numbered standards are to be utilized by the assessor to “assess to” and will be used by the FSIVA assessor as a guide in the conduct of the DoD CIP FSIVA. Specific Combatant Command, Service, and Agency missions will dictate which references and recommendations may apply to the numbered standards.

### 6.0 USE OF THE CIP CAPABILITY AREA STANDARDS

The standards provided in this document are applicable to vulnerability assessments that are conducted only on designated critical assets and any additional critical assets that may be subsequently identified as a result of a FSIVA. This document is intended for use by both the designated FSIVA assessors and the critical asset owners. In general, these standards will be used to:

## **For Official Use Only**

### **Draft CIP FSVA Standards**

- a. Establish the overarching baseline set of assessment requirements for critical assets to assist in the protection of these identified and validated critical assets.
- b. Establish the different areas of concern and associated assessment standards that a FSIVA will examine during an assessment.
- c. Assist in the training and certification of FSIVA assessors.
- d. Provide an overarching guide to help create and appropriately structure checklists for the assessment of designated DoD critical assets.

The FSIVA within the CIP capability area is intended to take a “modular” approach to conducting a vulnerability assessment of a designated critical asset. The assessment will be specifically tailored to accommodate the type of critical asset that is being assessed. For example, if a chemical storage site is designated as a critical asset, the assessment will look at those “*areas of concern*” that apply to that particular asset. Some of the areas of concern that could pertain to this example are Physical Security, Chemical Security, Personnel/Industrial Security, Safety, Plans and the Supporting Infrastructure.

Depending upon the nature of the critical asset to be assessed, several of the assessment areas of concern and assessment topic and sub topic areas may overlap. Overlapping areas and redundancies have been resolved to the extent possible during the development of this version of the document. An understanding of the critical asset environment and the assessment intent and context will help the assessor to determine the applicability of potentially redundant or overlapping areas. It is important to note that the standards for the Physical Security area of concern are the one set of standards that will apply to almost every type of asset that is being assessed. In addition, there are several other areas of concern that could be applicable to most types of assets that will be assessed. These areas of concern are Information Security, Personnel/Industrial Security, Plans, Supporting Infrastructure and Availability of Supporting Materiel and Services.

## **7.0 UNDERSTANDING THE EVOLVING CIP ENVIRONMENT**

As the CIP environment continues to evolve, the nature of threats to critical infrastructure will change, and the capabilities of threat individuals and groups will increase with the adoption of new technologies. The technology of security countermeasures will also continue to evolve in response to the changing threats. Most significant, perhaps, is the possibility that critical assets themselves will change as technology advances and the emergence of new infrastructure systems, especially communications systems, fosters system redundancies that make formerly designated

**For Official Use Only**  
**Draft CIP FSVA Standards**

critical assets no longer “critical”. At the same time, new technologies and newly identified critical assets will almost always carry their own vulnerabilities, the exploitation of which must be guarded against.

Because of this changing environment, the CIP capability area standards document is and will continue to be a “living” document. The baseline security standards for designated critical assets and the criteria for identifying and assessing the vulnerabilities of those assets will require periodic review and revision as the changes to the CIP environment dictate.

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

**PHYSICAL SECURITY**

**DESCRIPTION:**

That part of security concerned with physical measures designed to safeguard critical assets; to prevent unauthorized access to equipment, installations, materials, and documents that support critical assets; and to safeguard critical assets against espionage, sabotage, damage, and theft of critical assets.

<b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i>
<b><u>TOPIC:</u></b> <i>OUTER PERIMETER SECURITY</i>
<b><u>SUBTOPIC:</u></b> <i>PARKING</i>
<b><u>EXPLANATION:</u></b> Parking refers to methods employed to protect parking areas and control access to preclude entry by unauthorized vehicles from entering an area where a critical asset is located or an area adjacent to a critical asset.
<b><u>INTENT:</u></b> To prevent unauthorized vehicles and individuals from gaining access to parking areas located within close proximity to the critical asset.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Parking will include a review of measures to control and restrict access to parking areas in close proximity to critical assets. This will include a review of parking access controls; the use of parking permits and access decals; the assignment of parking areas; and the segregation of parking between government-owned, commercially owned, and privately owned vehicles.
<b><u>CRITERIA:</u></b> The standards for the assessment of Parking are based on guidelines contained in <i>Unified Facility Criteria (UFC) 4-010-10: Department of Defense (DoD) Minimum Antiterrorism Standards for Buildings (dated 31 July 2002)</i> , <i>DoD O-2000.12-H: Protection of DoD Personnel and Assets from Acts of Terrorism (dated October 2000)</i> , and <i>OPNAVINST 5530.14C: Navy Physical Security (dated 10 December 1998)</i> . These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.

## For Official Use Only

### Draft CIP FSVA Physical Security Standards

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether designated parking areas satisfy the facility/asset standoff requirements for security purposes.
  - ◆ *It is recommended that the designation of parking areas will take into account and will not infringe upon the facility/asset standoff requirements.*
2. The assessor must verify whether procedures and restrictions regarding parking beneath facilities containing critical assets, is conducive to assuring an appropriate level of security.
  - ◆ *It is recommended that parking beneath facilities that contain critical assets or on rooftops of facilities containing critical assets will be eliminated. Where very limited real estate makes such parking unavoidable, additional access control and structural measures to achieve an equivalent level of protection will be incorporated.*
3. The assessor must verify whether access controls for vehicular parking near facilities that house critical assets are adequate.
  - ◆ *It is recommended that access controls for vehicular parking will ensure vehicles are not allowed to park closer to the facility that houses the critical asset than the required standoff distance.*
4. The assessor must verify whether visitor parking procedures and restrictions outside the perimeter of the facility housing the critical asset are conducive to assuring an appropriate level of security.
  - ◆ *It is recommended that visitor-parking procedures be established outside the perimeter of the facility housing the critical asset. If this is not possible, visitor parking should be restricted to an observable area that is no closer to the facility than the required standoff distance.*
5. The assessor must verify whether parking procedures and restrictions within the critical asset perimeter are conducive to assuring an appropriate level of security.
  - ◆ *It is recommended that all parking procedures and restrictions within the critical asset perimeter be limited to employees.*
6. The assessor must verify whether procedures and restrictions for parking on streets directly adjacent to critical asset structures are conducive to assuring an appropriate level of security.
  - ◆ *It is recommended that parking on streets directly adjacent to critical asset structures not be permitted.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>OUTER PERIMETER SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>STANDOFF/SETBACK</i></p>
<p><b><u>EXPLANATION:</u></b> Perimeter Standoff/Setback refers to the distance measured from the exterior face of a critical asset or facility to those points at which vehicles and pedestrians are precluded from approaching the asset or facility further without proper authorization. Standoff is the second tier of defense. As a rule, the earlier the detection of threats and the longer the range at which they are detected, the greater the opportunities are to protect critical assets and minimize the impact of terrorist acts and threats against critical assets.</p>
<p><b><u>INTENT:</u></b> The primary design strategy is to ensure that any threats and unauthorized individuals are kept as far away from inhabited critical assets as possible or practical. Maximizing standoff distance also ensures that there is opportunity in the future to upgrade resources to meet increased threats or to accommodate higher levels of protection. Standoff zones provide time delays and more importantly, abatement of blast effects.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Standoff/Setback distances are based on a specific range of assumed threats that provides a reasonable baseline for the design of all inhabited locations that store critical assets. The assessment will review the levels of protection for vehicle bombs, waterborne vessel bombs, placed bombs, mail bombs, direct/indirect fire weapons; Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) materials; controlled/no controlled perimeter; standoff distances and separation for expeditionary and temporary structures; the construction design for the minimum standoff distances; and effective standoff distance.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Standoff/Setback are based on guidelines contained in <i>OPNAVINST 5530.14: Navy Physical Security (dated 10 December 1998)</i>, <i>UFC 4-010-10: DoD Minimum Antiterrorism Standards for Buildings (dated 31 July 2002)</i>, <i>Department of Defense Instruction (DoDI) 2000.18: Department of Defense Installation Chemical, Biological, Radiological, Nuclear and High Yield Explosive Emergency Response</i></p>

## For Official Use Only

### Draft CIP FSVA Physical Security Standards

*Guidelines (dated 4 December 2002) and Defense Threat Reduction Agency (DTRA): Antiterrorism Vulnerability Assessment Team Guidelines (dated October 2001).* These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether security personnel exercise proper security methods to mitigate threats to a critical asset.
  - ◆ *It is recommended that in order to mitigate the effectiveness of a vehicle bomb attack or other threats to a critical asset, security personnel and managers will be continually vigilant against allowing vehicle parking near high-density buildings and on piers. Every attempt should be made to establish minimum standoff distances, which vary depending on the type of construction, level of protection desired, and proximity of perimeter barriers.*
2. The assessor must verify whether standoff distances between the facility perimeter and primary gathering structures, including parking areas, vehicle access, and occupied buildings, are adequate to ensure an appropriate level of security. The assessor should consider the appropriate use, type of construction, population of the building, and whether it meets requirements in UFC Standards.
3. The assessor must verify whether perimeter standoff has a perimeter that precludes vehicles from reasonable access (e.g., perimeter fence, woods, berms, ditches, farm fields without access roads, guards, etc.).
4. The assessor must verify whether expeditionary and temporary structures that house critical assets are located away from public roads or other uncontrolled areas.
5. The assessor must verify whether exterior doors are positioned adequately so they cannot be easily targeted from the facility perimeter or uncontrolled vantage points.
6. The assessor must verify whether facilities that house critical assets, avoid conditions that would obscure packages from view near the building.
7. The assessor must verify whether adjacent land use has been adequately evaluated to determine the need for obscuration screening or additional measures necessary to preclude reasonable access.
8. The assessor must verify whether standoff for structures where critical assets reside, including parking areas and vehicle access, is appropriate to the use and type of construction and meets requirements in UFC.

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- |   |
|---|
| <p>9. The assessor must verify whether trash containers and other containers that could conceal an Improvised Explosive Device (IED) are located at an acceptable distance from the building housing the critical asset.</p> <ul style="list-style-type: none"><li>◆ <i>It is recommended that trash containers and other container that could conceal an IED are located at least 33 feet away from the building housing the critical asset.</i></li></ul> <p>10. The assessor must verify whether expeditionary and temporary structures where critical assets reside are properly isolated from functions requiring frequent vehicle access.</p> <ul style="list-style-type: none"><li>◆ <i>It is recommended that expeditionary and temporary structures housing critical assets be properly separated from mail and supply handling areas.</i></li></ul> |
|---|

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>OUTER PERIMETER SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>PROXIMITY TO HIGH-VALUE TARGETS</i></p>
<p><b><u>EXPLANATION:</u></b> To ensure that facilities/locations in the general area of the asset that could be the intended target of a threat are addressed and identified.</p>
<p><b><u>INTENT:</u></b> To ensure that other potential high-value targets in the general area of the asset are identified and the potential impact of an undesirable event directed against the target is anticipated and planned for.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of security procedures will include a review of potential high-value/high-threat targets in the vicinity of the asset being assessed. The impact on the asset should the high-value/high-threat target be exploited by threats will be identified.</p>
<p><b><u>CRITERIA:</u></b> Where specific documentary sources of assessment guidelines are not identified, as in the case of Proximity to High Value Targets, standards for assessment (listed below) are based on an analysis of findings and lessons learned from vulnerability assessments of a variety of government department and agency facilities and assets.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether there are high-value/high-threat targets within an unacceptable distance of the asset.<ul style="list-style-type: none"><li>◆ <i>It is recommended that high-value /high-threat targets within 15 miles of a critical asset are identified.</i></li></ul></li><li>2. The assessor must verify whether security managers of critical assets have conducted appropriate analysis to determine the potential likelihood that high-value/high-threats target will be exploited.</li><li>3. The assessor must verify whether physical security procedures and emergency response planning are in place and adequate to respond to an attack on the adjacent high-value target.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

4. The assessor must verify whether coordination with local responders (e.g., fire, police, etc.) to ensure that response support or access to the critical asset will not be adversely affected or interrupted if the other potential high-value target is exploited.
- ◆ *It is recommended that coordination is conducted with local responders (e.g., fire, police, etc.) to ensure that response support or access to the critical asset will not be adversely affected or interrupted if the other potential high-value target is exploited. This may involve the establishment of a Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA) with responders from other jurisdictions if local responders will be unable to commit.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>OUTER/INNER PERIMETER, SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>MONITORING</i></p>
<p><b><u>EXPLANATION:</u></b> Monitoring refers to the use of Closed-Circuit Television (CCTV), various types of Intrusion Detection Systems (IDS), and emergency detection and suppression systems (e.g., fire Hazardous Materials (HAZMAT), etc.) to observe and record activity in and around critical assets.</p>
<p><b><u>INTENT:</u></b> To help preclude unauthorized access to critical assets, to observe and record incidents of surreptitious activity for use in subsequent investigations, and to assist security forces in continuously monitoring areas that are near and/or around critical assets.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Monitoring will include a review of monitoring systems employed to observe and record individuals or incidents that occur in areas directly surrounding the critical asset, any entrances and exits, parking areas, delivery docks, and sensitive compartmented areas internal to the critical asset. Monitoring systems include CCTV, IDS, and fire detection and suppression systems.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Monitoring are based on from guidelines contained in <i>DTRA Antiterrorism Vulnerability Assessment Team Guidelines (dated October 2001)</i>, <i>United States (U.S.) Department of Justice (DOJ) Vulnerability Assessment of Federal Facilities (dated 28 June 1995)</i>, <i>DoD O-2000.12H: Protection of DoD Personnel and Assets from Acts of Terrorism (dated October 2000)</i> and <i>OPNAVINST 5530.14C: Navy Physical Security (dated 10 December 1998)</i>. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p>
<p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether fire detection and suppression systems satisfy detection, suppression, alarm, communication, and recording requirements.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- ◆ *It is recommended that the fire detection and suppression system includes alarms in all critical areas linked to a communications center equipped with fire alarm monitoring, communication and recording devices. The equipment should include all fire reporting telephone circuits, direct lines and the intra-base radio master control.*
- 2. The assessor must verify whether life-safety systems such as door panic hardware, exit lights, emergency lights, and fire extinguishers are installed and properly maintained.
- 3. The assessor must verify whether IDS has been sufficiently safeguarded against tampering so as to generate a prompt security force response when the systems are activated.
- 4. The assessor must verify the location of all sensors, transmitters, transponders, control units, and other IDS components associated with a protected zone is adequate to ensure that secure areas are protected by sensors that will detect tampering.
- 5. The assessor must verify whether IDS is supported by an emergency power source.
- 6. The assessor must verify whether surveillance systems and procedures are in place and sufficient in assuring appropriate levels of security.
  - ◆ *It is recommended that an integrated 24-hour CCTV system will be in place to monitor key areas of the critical asset.*
  - ◆ *It is recommended that time-lapse recording of the CCTV system will be used to monitor critical assets.*
  - ◆ *It is recommended that warning signs be posted advising CCTV surveillance is being conducted.*
  - ◆ *It is recommended that emergency communication systems (e.g., intercom, telephones, etc.) will be installed at easily identifiable, well-lit, CCTV-monitored locations to permit employee's direct contact with security personnel.*
  - ◆ *It is recommended that CCTV cameras capable of displaying and recording activity in the parking area will monitor parking lots.*
  - ◆ *It is recommended that detection equipment capable of detecting chemical agents, biological agents, and radioactivity will be installed and monitored.*
  - ◆ *It is recommended that the installation will ensure the maintenance of the detection systems is occurring quarterly by a certified technician.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>OUTER PERIMETER SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>PHYSICAL BARRIERS</i></p>
<p><b><u>EXPLANATION:</u></b> Physical Barriers refers to those devices designed to control, deny, impede, and discourage access by unauthorized persons to a critical asset.</p>
<p><b><u>INTENT:</u></b> To assist in the protection of critical assets by denoting the perimeters that surround critical assets and inhibiting access to facilities by unauthorized persons and vehicles.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Physical Barriers will include a review of the current deployment of physical barriers to control, deny, impede, and discourage access by unauthorized persons to a critical asset. The types of barriers available can be broken down into structural (e.g., fences, walls, doors, etc.) and natural (e.g., mountains, swamps, vegetation, etc.).</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Physical Barriers are based on guidelines contained in <i>OPNAVINST 5530.14C: Navy Physical Security (dated 10 December 1998)</i>, <i>DoD O-2000.12-H: Protection of DoD Personnel and Assets from Acts of Terrorism (dated October 2000)</i> and <i>DTRA Antiterrorism Vulnerability Assessment Team Guidelines (dated October 2001)</i>. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether physical barriers have been established along the designated perimeter of all areas where critical assets reside and provides an acceptable degree of continuous protection.<ul style="list-style-type: none"><li>◆ <i>It is recommended that physical barriers be established along the designated perimeter of all areas where critical assets reside. The barrier or combination of barriers used affords a minimally acceptable degree of continuous protection along the entire perimeter of the critical asset area.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

2. The assessor must verify whether fences are at an acceptable height and of adequate construction so that it prevents the fence from being manipulated to gain surreptitious entry.
  - ◆ *It is recommended that fences are high enough to prevent the fence from being lowered by pulling down on the top of the fence material.*
  - ◆ *It is recommended that the bottom of the fence material will be close enough to firm soil or buried sufficiently to prevent surreptitious entry under the fence.*
  - ◆ *It is recommended that culverts under or through a fence will be secured to prevent their use for surreptitious entry.*
  - ◆ *It is recommended that fences will be located so that the features of the land (i.e., its topography) or structures (e.g., buildings, utility tunnels, etc.) do not aid passage over, around, or under the fence.*
  - ◆ *It is recommended that fence materials be reinforced to improve resistance to penetration, as appropriate, based on the assessed level of threat, the potential impact of asset loss, and the presence and effectiveness of other supporting countermeasures.*
3. The assessor must verify whether the protection afforded by walls is sufficient to ensure the protection of the critical asset.
  - ◆ *It is recommended that the protection afforded by walls is equivalent to that provided by chain link fencing.*
  - ◆ *It is recommended that the assessor refer to DoD O 2000.12 H, Chapter 9 for details on the specifications on walls used as physical barriers.*
  - ◆ *It is recommended that that the assessor refer to DoD O 2000.12 H, Chapter 9 and OPNAVIST 5530.14 C, Chapter 6 for details on specifications on clear zones, specifically, the specifications on walls used as physical barriers.*
4. The assessor must verify whether security force personnel check restricted area perimeter barriers and clear zones for defects that would facilitate unauthorized entry and report such defects to supervisory personnel.
  - ◆ *It is recommended that personnel be alert for the following:*
    - *Damaged areas*
    - *Deterioration*
    - *In the clear zones that would afford cover for possible intruders and concurrently hinder the effectiveness of any protective lighting, assessment systems.*
    - *Obstructions that would afford the concealment or aid entry/exit for an intruder or provide a plausible excuse to openly loiter without need for hiding (e.g., bus stop next to fence line, etc.).*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

5. The assessor must verify whether Restricted Area Perimeter Openings are sufficiently addressed and monitored to ensure continued operations and protect against surreptitious entry.
  - ◆ *It is recommended that openings in the perimeter barrier are kept at the minimum necessary for safe and efficient operation of the activity.*
  - ◆ *It is recommended that access through such openings is either controlled, secured against surreptitious entry or other compensatory measures.*
  - ◆ *It is recommended that these openings be inspected frequently by security patrols.*
6. The assessor must verify whether sufficient procedures for the use Vehicle Barriers are in place to prevent unauthorized vehicle access.
  - ◆ *It is recommended that the use of vehicle barriers such as crash barriers, obstacles, or reinforcement systems for chain link gates at controlled avenues of approach impede or prevent unauthorized vehicle access.*
7. The assessor must verify whether sufficient procedures for the use of Permanent Structures as perimeters are in place to ensure the protection of the facility housing a critical asset.
  - ◆ *It is recommended that several permanent structures be used as perimeters around an entire facility, around enclaves within a facility, or around an isolated building used solely to house critical assets.*
  - ◆ *It is recommended that several permanent structures be used as perimeters around an entire facility, around enclaves within a facility, or around an isolated building used solely to house critical assets.*
  - ◆ *It is recommended that bollards or other barricades be considered for this purpose. These should be less than 3 feet in height and installed at the base of the wall to increase standoff distance between parked vehicles and the wall to at least 10 feet.*
8. The assessor must verify whether temporary barriers are employed where permanent barriers are planned for but not installed or where evolving conditions warrant additional short-term protection for critical assets.
  - ◆ *It is recommended that vegetation barriers should include hedges that are thick and covered with thorns or pointed leaves.*
  - ◆ *It is recommended that portable fencing can be used as a temporary perimeter to establish psychological barriers and to channel pedestrian and vehicle movement.*
9. The assessor must identify whether sufficient temporary walls/rigid barriers are used to ensure protection of the critical asset.

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- ◆ *It is recommended that these temporary walls/rigid barriers be installed along approaches to sites or facilities within boundaries to force vehicles to make tight, slow turns before approaching gates or building entrances. Options include concrete vehicle barriers (Jersey wall segments), concrete or sand filled oil drums, concrete bollards/planters, steel or steel reinforced concrete posts, or vehicles in all sizes and configurations parked bumper to bumper.*
10. The assessor must verify whether the facility has an executable barrier plan and sufficient resources to implement the plan.
  11. The assessor must verify whether vehicle entrances are capable of stopping a vehicle threat or sufficiently impeding the vehicle to allow for security force response.
    - ◆ *It is recommended that head on vehicular approaches be eliminated for primary gathering structures.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>PERIMETER SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>EXTERIOR SECURITY LIGHTING</i></p>
<p><b><u>EXPLANATION:</u></b> Exterior Security Lighting refers to the level of illumination for the exterior of critical assets/facilities.</p>
<p><b><u>INTENT:</u></b> To ensure that sufficient exterior security lighting exists to discourage or deter attempts at entry by intruders, make detection likely if entry is attempted, and prevent glare that may temporarily blind security personnel. Effective exterior lighting also assists first responders in the event of fire or other emergencies during periods of darkness or reduced visibility.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Exterior Security Lighting will include an evaluation of perimeter lighting positioning, illumination of exterior doors, the adequacy of lighting to assist security personnel, illumination of parking areas, illumination of all approaches to any critical assets, use of lighting to support CCTV, unnecessary illumination, location of lighting control systems, and emergency back-up power for lighting systems.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Exterior Security Lighting are based on guidelines contained in <i>DoD 2000.12-H: Protection of DoD Personnel and Assets from Acts of Terrorism (dated October 2000)</i>, <i>AFI 31-101: The Air Force Installation Security Program (dated 1 June 2000)</i> and <i>FM 19-30: Physical Security (dated 8 January 2001)</i>. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p>
<p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify that sufficient protective lighting has been installed for the purpose of assuring appropriate levels of security.<ul style="list-style-type: none"><li>◆ <i>It is recommended that in planning protective lighting procedures, high-brightness contrast between intruder and background will be the first consideration.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

2. The assessor must verify whether sufficient protective lighting is achieved through uniform lighting of the perimeter areas surrounding the critical asset.
3. The assessor must verify whether building face perimeter lighting is sufficient to illuminate the faces of buildings on or within an acceptable distance of the property line or the area line to be protected and where the public may approach the building.
  - ◆ *It is recommended that building face perimeter lighting is sufficient to illuminate the faces of buildings on or within 20 feet of the property line or the area line to be protected and where the public may approach the building.*
4. The assessor must verify whether active entry lighting for pedestrians and vehicles is sufficient to provide for positive recognition of persons, examination of credentials, and inspection of vehicles including their contents and passengers.
5. The assessor must verify whether power generators, transformers, fixtures, and hardware associated with the lighting system are contained within the perimeter of the facility housing the critical assets or otherwise protected.

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

**AREA OF CONCERN:**

*PHYSICAL SECURITY*

**TOPIC:**

*PERIMETER SECURITY*

**SUBTOPIC:**

*SECURITY FORCE OPERATIONS (SFO)*

**EXPLANATION:**

Security Force Operations (SFO) refer to those designated persons specifically organized, trained and equipped to provide physical security and law enforcement support to a critical asset. Security forces may include military units, non-military DoD police and other police agencies or contracted security force personnel.

**INTENT:**

To ensure that security forces are appropriately staffed, equipped and trained to enforce laws and regulations, deter and detect terrorism and criminal activities, prevent/deter theft and losses caused by fire damage, accidents, trespass, sabotage, and espionage directed against a critical asset.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of SFO that protect critical assets will include assessing the security forces, security force augmentation program and the adequacy of equipment and resources available for use by both regular and augmented security personnel. It is important their tasks and responsibilities are clearly defined and the command and control of these forces be understood throughout the site. Jurisdiction and rules of engagement will be clearly identified in the site plan. This portion of the assessment will focus on their contribution to the physical security program to deter, detect, delay, and respond to threats. Additionally, security force training and exercises are key areas to be reviewed. The following criteria will include waterside and physical security program issues as applicable.

**CRITERIA:**

The standards for the assessment of SFO are based on guidelines contained in *DTRA Antiterrorism Vulnerability Assessment Team Guidelines (dated October 2001)*, *DoD 2000.16: DoD Antiterrorism Standards (dated 14 June 2001)* and *DoD O-2000.12H: Protection of DoD Personnel and Assets from Acts of Terrorism (dated October 2000)*. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether the security force-training program ensures that all personnel including personnel assigned to the augmentation security force are able to perform routine duties competently and meet emergencies quickly and efficiently.
2. The assessor must verify whether security forces are equipped with sufficient equipment, both type and quantity, including weapons; ammunition; effective communications equipment including secure, personal protective equipment; and vehicles.
3. The assessor must verify whether specialized support will be available for security operations. Support consists of explosive ordnance disposal, bomb detection, Security Response Teams (SRTs), negotiators, interpreters, hazardous material, etc.
4. The assessor must verify whether security forces responsible for maritime security operations are properly trained to perform these duties.
  - ◆ *It is recommended that personnel should also be trained and certified/licensed to operate patrol craft. They should also be trained in navigation and port security tactics, including patrol techniques, intercept procedures, defensive boat tactics, and boarding.*
5. The assessor must verify whether exercises are conducted with both the regular security force and the augmentation force.
6. The assessor must verify whether written instructions/post orders are established and distributed to all security force posts.
  - ◆ *It is recommended that these instructions/orders will identify duties and responsibilities under all threats.*
7. The assessor must verify whether security forces have established liaison with local law enforcement/host nation security forces.

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>PERIMETER SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>ACCESS CONTROL</i></p>
<p><b><u>EXPLANATION:</u></b> Access Control refers to a system or procedure established to prevent unauthorized entry or access to a critical asset.</p>
<p><b><u>INTENT:</u></b> To ensure that effective access control procedures are in place to preclude access by unauthorized individuals and to prevent the introduction of harmful devices, materiel and components to a critical asset. Access control measures for vehicular, pedestrian, watercraft, or aircraft will be evaluated to determine the effectiveness of the system or procedure to positively identify those entering the perimeter and prevent unauthorized entry or the introduction of explosives and other weapons. Access control measures minimize the misappropriation; pilferage or compromise of material; or recorded information pertaining to critical assets by controlling personnel, packages, vehicles, vessels, material, and property movement.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Access Control will include assessing the measures that are in place to prevent unauthorized access to and provide protection of critical assets. This will include examining the measures that are currently in place to control movement in port to prevent unauthorized vessels from coming within 50 yards of United States (U.S.) ships. This will also include measures to prevent unauthorized aircraft from critical asset restricted airspace, vehicle access control points, pedestrian access control points, monitoring systems/detection aids, security forces post orders, and standard operating procedures. Access-control rosters, personnel recognition, identification cards, badge exchange procedures, and personnel escorts will all contribute to an effective access control system.</p>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

**CRITERIA:**

The standards for the assessment of Access Control are based on guidelines contained in DoD 02000.12-H: *Protection of DoD Personnel and Assets from Acts of Terrorism* (dated October 2000), OPNAVINST 5530.14C: *Navy Physical Security* (dated 10 December 1998), FM 19-30: *Physical Security* (dated 8 January 2001), AR 190-13: *The Army Physical Security Program* (dated 30 September 1993), and/or based on DTRA Antiterrorism Vulnerability Assessment Team Guidelines (dated October 2001). These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

**General Access Control:**

1. The assessor must verify whether primary access to a critical asset has security personnel present during peak traffic periods and automated systems for remote operations during other periods.
2. The assessor must verify whether the methods used to control personnel access to a critical asset are included in written procedures in the facility's physical security plan.
  - ◆ *It is recommended that the following personnel access information should be included in the facility's physical security plan:*
    - *Description of access control methods used.*
    - *Methods for establishing appropriate authorization for entering and leaving the asset, or any area within the asset requiring special access protocols, as they apply to both personnel continually authorized access to the area and to visitors, including an special provisions concerning non duty hours.*
    - *Details of where, when and how security badges are displayed.*
    - *Procedures to cover issued security badges.*
    - *Procedures to be followed in case of loss or damage to security badges.*
    - *Procedures to recover issued security badges.*
    - *Measures to deny illicit use of lost, stolen, or illegally acquired security badges.*
3. The assessor must verify whether procedures and restrictions for vehicle entry to a facility that contains a critical asset are sufficient.
  - ◆ *It is recommended that when authorized vehicles enter a facility that contains a critical asset, they undergo a systemic search, including, but not limited to the following:*
    - *Vehicle Interior*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- *Engine Compartment*
  - *External Air Breathers*
  - *Top of Vehicle*
  - *Battery Compartment*
  - *Cargo Compartment*
  - *Undercarriage*
4. The assessor must verify whether sufficient pedestrian screening procedures are conducted.
- ◆ *It is recommended that pedestrian screening be conducted between the visitor parking area and other sections of the facility.*
5. The assessor must verify whether sufficient access control for ports is performed.
- ◆ *It is recommended that a security zone be established within the surveillance area extending from the high-water mark to a distance at least 1,000 meters from shore if possible.*
6. The assessor must verify whether visitor control procedures have been established and are properly followed at the facility/installation.
- ◆ *It is recommended that security force or reception staff contact the person or activity being visited to verify the visitor's identity visit requirement. Once verification is accomplished, a visitor's badge will be issued, a registration form will be completed, and an escort will be assigned before allowing visitors access to facilities housing critical assets.*
  - ◆ *It is recommended that the procedures for admitting Very Important Persons (VIPs) and foreign nationals into facilities housing critical assets should be clearly articulated in security force post orders. A 24-hour advance notice will be required for these requests, along with an agenda for the visit and designation of an escort.*
  - ◆ *It is recommended that to allow civilians on jobs under government contracts to conduct business in facilities housing critical assets, the security manager will coordinate with the procurement office to ensure appropriate background checks have been conducted and there is a stated need for access. The security manager will also identify movement control procedures for these employees.*
  - ◆ *It is recommended that supervisors using cleaning teams will seek technical advice from the physical security office on internal controls for each specific building. This will include procedures for providing escorts.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- ◆ *It is recommended that supervisors establish internal controls for employees in work areas after normal operating hours based on coordination with the security manager. Supervisors should notify security personnel of the worker's presence and duration of work.*
7. The assessor must verify whether procedures regarding the issuance of security identification cards and badging control are being followed at the facility.
- ◆ *It is recommended that specifications for security identification cards and badges include the following:*
    - *Cards and badges will identify the name of the facility for which they are valid.*
    - *Cards and badges will show the name and photograph of the person to whom it is issued. Visitor cards and badges will show "Visitor" in place of name and photograph, and will have "Escort Required" or "No Escort Required" printed across the face of the badge as appropriate.*
    - *Cards and badges issued for the areas housing the critical asset will show an expiration date.*
    - *Cards and badges will identify the areas for which they are valid.*
8. The assessor must verify whether control and storage procedures for security identification cards and badges are sufficiently established and followed.
- ◆ *It is recommended that the responsible authority establish detailed procedures controlling the issue, turn in, recovery, and expiration of security identification cards and badges.*
  - ◆ *It is recommended that engraved plates and all printed or coded parts of the cards and badges, although unclassified, will be handled and stored the same as CONFIDENTIAL material. The source of cards and badges will be controlled to prevent use by and distribution to unauthorized persons.*
  - ◆ *It is recommended that mutilated or defective cards and badges, and those discharged or transferred personnel, will be treated as CONFIDENTIAL material until destroyed.*
  - ◆ *It is recommended that lost cards and badges will be invalidated promptly.*
  - ◆ *It is recommended that cards and badges that allow access to the critical asset will be replaced at intervals determined appropriate by the responsible authority.*
  - ◆ *It is recommended that security personnel limit the issue of badges to those with need, by category (e.g., employee, contractor, etc.).*
  - ◆ *It is recommended that security personnel ensure continuous accountability of all issued badges.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- ◆ *It is recommended that security personnel identify lost or unaccounted for badges immediately.*
- ◆ *It is recommended that security personnel take action to cancel lost/unaccounted for badges or reissue all badges as appropriate to the access badge/card system in use.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>PERIMETER SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>ENTRANCES AND EXITS</i></p>
<p><b><u>EXPLANATION:</u></b> Entrances and Exits refer to physical security measures employed to properly protect critical asset entry points from surreptitious entry.</p>
<p><b><u>INTENT:</u></b> To ensure that entrances and exists to critical assets are sufficiently controlled so as to protect the asset from damage, loss or compromise.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Entrances and Exits will include a review of all entrance/exit points, methods to harden and secure entry/exit points to deter, detect, and delay intruders from gaining access to critical assets.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Entrances and Exits are based on guidelines contained in <i>UFC 4-010-10: DoD Minimum Antiterrorism Standards for Buildings (dated 31 July 2002)</i> and <i>DoD O-2000.12-H: Protection of DoD Personnel and Assets from Acts of Terrorism (dated October 2000)</i>. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether main facility entrances and exits are situated effectively to preclude direct line of sight viewing from the facility perimeter or other uncontrolled vantage points.</li><li>2. The assessor must verify whether all exterior doors into inhabited areas open outward to facilitate emergency evacuation and to mitigate the effects of an explosion.</li><li>3. The assessor must verify whether access to rooftop doors and entranceways is effectively controlled to minimize the possibility of surreptitious entry.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- ◆ *It is recommended that where possible, external rooftop access be eliminated through the use of internal access ways and by security existing external ladders and stairways.*
4. The assessor must verify whether the materials used in the construction of exterior windows, doors, and mullions is sufficient to protect against surreptitious entry and mitigate the effects of an explosion.
    - ◆ *It is recommended that a minimum of 6 mm (1/2 inch) nominal laminated glass be used for all exterior windows and glazed doors. Doors, window frames, and mullions should be constructed of aluminum or steel.*
  5. The assessor must verify whether the number of exterior doors has been limited to the minimum necessary for emergency evacuation.
  6. The assessor must verify whether normal entry will be restricted to a single entranceway when threat conditions dictate.
  7. The assessor must verify whether high-security locking systems are used on all doors.
    - ◆ *It is recommended that if more than one door exists, only one should be equipped with outside mounted locks and entry hardware.*
    - ◆ *It is recommended that externally mounted locks and hasps on utility areas will be replaced with internally locking devices and hinges that are positioned to reduce their vulnerability to tampering.*
    - ◆ *It is recommended that double doors opening out should be equipped with protected hinges and a lock that is key operated from both sides. The inactive half of the double door should be equipped with flush throw bolts with at least 1½-inch penetration at the head and foot of the door.*
  8. The assessor must verify whether proper methods and procedures for securing utility openings/access points are followed at the facility/installation.
    - ◆ *It is recommended that the assessor refer to DoD O 2000.12 H, Chapter 10 for details on the proper methods and procedures for securing utility openings/access points.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

**AREA OF CONCERN:**

*PHYSICAL SECURITY*

**TOPIC:**

*PERIMETER SECURITY*

**SUBTOPIC:**

*RECEIVING AND SHIPPING*

**EXPLANATION:**

Receiving and Shipping refers to those policies, procedures, and practices designed to protect critical assets for the introduction of hazardous devices or materials and to protect critical assets in transit. Security control measures for incoming and outgoing mail, packages, equipment, and resources that are vital to national security will be in place.

**INTENT:**

To ensure that all deliverable goods are screened and cleared for safe transport in and out of controlled and/or restricted zones that are located near critical assets in an effort to prevent explosive or other hazardous devices from being delivered.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of Receiving and Shipping refers to measures of control, plans and procedures to ensure all items received and transported do not present a threat to critical assets. Included will be screening and searches of these goods, in-processing and storage, proper storage facilities, and associated equipment and handling procedures for detection of explosives, toxic leaks, and/or undesirable events as a result of improper receiving and shipping procedures.

**CRITERIA:**

The standards for the assessment of Receiving and Shipping are based on guidelines contained in *U.S. DoD Vulnerability Assessment of Federal Facilities (dated 28 June 1995)*, *UFC 4-010-10: DoD Minimum Antiterrorism Standards for Buildings (dated 31 July 2002)*, *DTRA Antiterrorism Vulnerability Assessment Team Guidelines (dated October 2001)*, *AR 190 XX: Biological Agent Security Program (Draft)* and *AR 190-59: Chemical Agent Security Program (dated 1 July 1998)*. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.

## For Official Use Only

### Draft CIP FSVA Physical Security Standards

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether packages entering buildings where critical assets reside are subject to X-ray screening and/or visual inspection by security personnel.
2. The assessor must verify whether mailrooms are located an acceptable distance from critical assets and critical infrastructure.
  - ◆ *It is recommended that mailrooms be located as far from critical assets and critical infrastructure as possible.*
3. The assessor must verify whether acceptable mail and parcel handling procedures are being followed.
  - ◆ *It is recommended that mail and parcel handling procedures include screening, delivery and response for expected explosive devices.*
4. The assessor must verify whether mail handlers are properly trained in identifying mail and parcel bombs and whether exercises are being conducted to ensure personnel remain trained and alert.
5. The assessor must verify whether a central screening point has been established for all parcel deliveries.
  - ◆ *It is recommended that all deliveries be screened at this location.*
6. The assessor must verify whether there is an adequate system of package and material control in place.
  - ◆ *It is recommended that a system of package and material control be established. The system should be used to control movement of packages and materials into and out of the controlled area. Procedures should be established for inspecting for prohibited items and contraband. Sealed packages that cannot be inspected will require a signed property pass. The bearer of the sealed package will not be authorized to sign the property pass. Persons authorized to sign the property pass will be designated in writing by the appropriate authority. Samples of signatures of personnel authorized to sign property passes will be maintained at the entry/exit control point. Other packages and materials not covered by a property pass will be inspected for unauthorized items.*
7. The assessor must verify whether there is a sufficient positive system used to control movement of packages, material and vehicles into and out of areas housing critical assets.
  - ◆ *It is recommended that an electronic detection system should be used to enhance the controls. Searches and inspections for prohibited items and contraband will be conducted in accordance with AR 190 22.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

8. The assessor must verify whether responsible authorities have prescribed procedures to be followed when unauthorized items are found or when an individual refuses to be searched upon probable cause.
- ◆ *It is recommended that responsible authorities have prescribed procedures to be followed when unauthorized items are found or when an individual refuses to be searched upon probable cause.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>PERIMETER SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>CONSTRUCTION AND DESIGN</i></p>
<p><b><u>EXPLANATION:</u></b> Construction and Design refers to those measures taken to integrate security planning with asset design, to ensure that construction materials support the assets security requirements and to ensure that critical asset perimeters are hardened or reinforced as required to protect against all threats.</p>
<p><b><u>INTENT:</u></b> Effective construction and design measures will help ensure the integrity of the facility housing a critical asset.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Construction and Design will include a review of the plans and materials used in construction of existing and planned facilities that house critical assets and the integration of security countermeasures into those plans.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Construction and Design are based from guidelines contained in <i>DTRA Antiterrorism Vulnerability Assessment Guidelines (dated October 2001)</i> and <i>OPNAVINST 5530.14: Navy Physical Security (dated 10 December 1998)</i>. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether plans for new construction and/or existing building material have been reviewed to ensure additional protection is achieved when standoff requirements are not being met.<ul style="list-style-type: none"><li>◆ <i>It is recommended that when required standoff is not available at existing structures due to the close proximity to other buildings, plans for new construction and/or existing building material will be reviewed to ensure that additional protection is achieved.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- |  |
|--|
| <p>2. The assessor must verify whether new construction and renovation projects include a security review at all stages of planning, programming, design, and construction.</p> <ul style="list-style-type: none"><li>◆ <i>It is recommended that facility master plans, design guides, and architectural compatibility standards be reviewed for compatibility with established physical security standards, concerns, and guidelines within this document.</i></li></ul> <p>3. Where applicable, the assessor must verify whether applicable risks of progressive collapse have been established for a building housing a critical asset.</p> <ul style="list-style-type: none"><li>◆ <i>It is recommended that if a critical asset is located in a building that is three or more stories, the risks of progressive collapse should be established.</i></li></ul> |
|--|

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>INTERIOR SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>UTILITIES</i></p>
<p><b><u>EXPLANATION:</u></b> Utilities refer to the physical security of those electrical power; water; fuel; and Heating, Ventilation, and Air Conditioning (HVAC) system components that directly support the critical asset.</p>
<p><b><u>INTENT:</u></b> To ensure that utility systems components that directly support critical assets are safeguarded against sabotage, damage, and tampering.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Utilities that support the critical asset will include a review of access controls to those components of electric power, water, fuel, and HVAC systems that directly support the critical asset. This will include an examination of redundant utilities and support capabilities (e.g., back-up generator, reserve fuel, MOU/MOA with electrical power company, etc.) to ensure support in the event of primary components failure.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Utilities are based on guidelines contained in <i>DoDI 2000.16: DoD Antiterrorism Standards (dated 14 June 2001)</i>, <i>DOJ Vulnerability Assessment of Federal Facilities (dated 28 June 1995)</i>, <i>DTRA Antiterrorism Vulnerability Assessment Guidelines (dated October 2001)</i> and <i>DoD O-2000.12H: Protection of DoD Personnel and Assets from Acts of Terrorism (dated October 2000)</i>. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. In the context of Electric Power, the assessor must verify the following:<ol style="list-style-type: none"><li>a. The assessor must verify whether the facility has identified the source of electric power to determine whether there is flexibility and redundancy (e.g., load shedding capabilities, multiple feeders, looped system, multiple switches, etc.).</li></ol></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- b. The assessor must verify whether the facility has determined the reliability of local generating equipment, the distribution system and mechanisms (e.g., procedures, Standard Operating Procedures (SOPs), MOUs, etc.) in place to support the facility in the event of a total or prolonged power outage.
  - c. The assessor must verify whether the location of the power generating facility has been evaluated for proximity to public access and susceptibility to a threat.
  - d. The assessor must verify whether the facility has determined the number and location of high voltage feeders supporting the base or any critical facility independently supported within the base (e.g., hospitals; Command, Control, and Communications (C3) facilities; etc.) when electric power is supplied from outside sources. The assessor must verify whether main feeders have been sufficiently secured and provided with physical security controls to prevent tampering or sabotage.
  - e. The assessor must verify whether critical infrastructure support elements are located an acceptable distance from electric substations to prevent or minimize multiple support systems from being destroyed simultaneously.
  - f. The assessor must verify whether the facility/installation has provided backup power (e.g., Uninterruptible Power Supply (UPS) and/or emergency generators, etc.) at critical facilities with enough capacity to support those facilities during prolonged periods of time.
  - g. The assessor must verify whether backup power units are being maintained and tested on a regular basis, fuel tanks for these units are being secured, and emergency generators are equipped with Automatic Transfer Switches (ATs).
  - h. The assessor must verify whether written contingency plans have been developed for power outages.
2. In the context of Water, the assessor must verify the following:
- a. The assessor must verify whether facilities have identified the source and reliability of the water supply and distribution system.
  - b. The assessor must verify whether the fire chief or the authority having jurisdiction for the facility has calculated the quantity of available water stored and supplied for emergency conditions to ensure that it is adequate for fighting fires.
  - c. The assessor must verify whether a comprehensive maintenance and capital improvement program includes the water distribution system.

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- d. The assessor must verify whether pumping stations, critical nodes, and valve pits are secured and provided with adequate physical security controls to prevent tampering or sabotage.
  - e. The assessor must verify whether the facility properly ensures that the water system is looped, the pressure is adequate, a flushing program is conducted to eliminate sediments, and valves are periodically exercised and maintained.
  - f. The assessor must verify whether the facility has identified alternate water sources.
  - g. The assessor must verify whether facilities have developed a written contingency plan for water outages.
3. In the context of Fuel, the assessor must verify the following:
- a. The assessor must verify whether the facility provides procedures for the delivery, storage and security of all fuels.
  - b. The assessor must verify whether the facility determines who is responsible for testing fuels for contaminants and the frequency in which testing is performed.
  - c. The assessor must verify the locations of fuel tanks and fuel distribution systems; whether they are above ground or underground; and their size, contents, and distance from occupied facilities.
  - d. The assessor must verify whether the facility has identified an acceptable location for fuel trucks to be parked in relation to high population buildings and critical infrastructure.
4. In the context of Communications, the assessor must verify the following:
- a. The assessor must verify whether a contingency plan exists to re-route communications in the event the main telephone exchange is lost.
  - b. The assessor must verify whether a redundant communication feed to the facility or an alternate system is available.
  - c. The assessor must verify whether all switches, Public Branch Exchange (PBX) and key systems connected to the main switch have power generation and UPS.
  - d. The assessor must verify whether UPS systems are maintained regularly and exercised.
  - e. The assessor must verify whether the telephone switch has adequate physical security measures in place to control access to the facility.

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- f. The assessor must verify whether all access points to the telephone switch cable vault and manhole covers are properly secured.
  - g. The assessor must verify whether the facility cable distribution system is designed in a looped configuration.
5. The assessor must verify whether air intakes are protected to prevent unauthorized access and introduction of threat agents and properly equipped to protect against airborne contaminants.
  6. The assessor must verify whether air intakes for a critical asset are at an appropriate height above ground level and/or provided with appropriate physical security measures to prevent the introduction of airborne contaminants.
  7. The assessor must verify whether the facility/installation ensures the maintenance of filter systems is occurring on a routine basis by trained technicians.
  8. The assessor must verify whether a building's exterior is routinely inspected to locate and remediate any utility openings.
    - ◆ *It is recommended that if possible the following openings should be eliminated: utility openings, manholes, tunnels, air conditioning ducts, filters, or equipment access panels to preclude a potential entry point.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>INTERIOR SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>LOCK/KEY CONTROL</i></p>
<p><b><u>EXPLANATION:</u></b> Lock/Key Control refers to devices and processes used to secure entrances and exits leading into areas associated with a critical asset.</p>
<p><b><u>INTENT:</u></b> To ensure that areas associated with critical assets that require locks and/or keys are strictly controlled and accounted for at all times.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Lock/Key Control will include a review of the procedures and practices for storing, issuing, periodically inventorying, receiving, and otherwise accounting for keys and locks. The review will also assess the practice for accounting for and replacing lost, stolen or damaged keys and periodically rotating locks and/or changing ciphers and combinations.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Lock/Key Control are based on guidelines contained in <i>AR 190-59: Chemical Agent Security Program (dated 1 July 1998)</i> and <i>AR 190-51: Security of Unclassified Army Property (1 July 1998)</i>. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether keys to installed locks on critical structures, buildings, rooms, IDS, gates, manhole covers, and their key containers are strictly controlled and accounted for at all times.<ul style="list-style-type: none"><li>◆ <i>It is recommended that these keys will be maintained separately from other keys and will be accessible only to those individuals whose official duties require access to them.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

2. The assessor must verify whether adequate locking procedures are followed to safeguard critical assets.
- ◆ *It is recommended that that U.S. Government key-operated, pin-locking deadbolts be used to safeguard critical assets.*
  - ◆ *It is recommended that keys required for maintenance and repair of IDS, should be accessible only to authorized maintenance personnel. A list of authorized maintenance personnel should be kept current and accessible to personnel who control such keys.*
  - ◆ *It is recommended that the number of keys be held to a minimum. Keys should not be duplicated unless authorized personnel duplicate keys. Duplicated keys should be strictly accounted for at all times.*
  - ◆ *It is recommended that when not attended or in use, keys should be secured in a locked container. Any General Services Administration (GSA) approved or equivalent container or key container of at least 26-gauge steel is acceptable for storing such keys.*
  - ◆ *It is recommended that the key storage container will be kept in a room where it is kept under 24-hour surveillance.*
  - ◆ *It is recommended that keys be inventoried jointly with each change of custody recorded.*
  - ◆ *It is recommended that keys and locks be inventoried by serial number each month.*
  - ◆ *It is recommended that key padlocks be changed and have their cylinders replaced or rotated randomly between critical asset sites or facilities at least every 12 months. This requirement also applies to padlocks on perimeter gates that do not have authorized keyed locks or padlocks on manhole covers that may permit entry to critical assets.*
  - ◆ *It is recommended that a primary and alternate key custodian will be designated in writing to issue and recover keys and to maintain accountability for all assigned keys.*
  - ◆ *It is recommended that the key custodian maintain an accurate accountability for all keys at all times.*
  - ◆ *It is recommended that keys be signed out to authorized personnel on a key control roster.*
  - ◆ *It is recommended that an investigation be conducted immediately in the event of lost, misplaced, or stolen keys and the affected locked cores be replaced immediately.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- ◆ *It is recommended that combinations to locks be changed annually, upon change of custodian or other person having knowledge of the combination, or when the combination has been subject to possible compromise. Combinations should also be changed when a container is first put into service.*
- ◆ *It is recommended that combinations be recorded, sealed in an envelope, and stored in a locked container.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>INTERIOR SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>COMPARTMENT AREA ACCESS</i></p>
<p><b><u>EXPLANATION:</u></b> Compartmented Area Access refers to systems designed to control access at all perimeter entrances to Sensitive Compartmented Information Facilities (SCIFs).</p>
<p><b><u>INTENT:</u></b> To ensure that compartmented access is controlled to prevent and detect unauthorized access to SCIFs supporting critical assets.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Compartmented Area Access will include a review of automated access control systems, non-automated access control systems, processes, and personnel requirements and restrictions.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Compartmented Area Access are based on the <i>Director of Central Intelligence Directive (DCID) 6/9: Physical Security Standards for Sensitive Compartments Information Facilities (dated 18 November 2002)</i>. This reference addresses all of the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether the automated personnel access control system verifies the identity of an individual by an acceptable method.<ul style="list-style-type: none"><li>◆ It is recommended that one of the following methods is used in the identification of individuals:<ul style="list-style-type: none"><li>➤ <i>An identification (ID) badge or card should identify to the access control system the individual to whom the card is issued. A Personal ID Number (PIN) should be required. The PIN should be separately entered into the system by each individual using a keypad device and should consist of four or more digits, randomly selected, with no known or logical association with the individual.</i></li></ul></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- *Personal identify verification (i.e., biometrics device) should identify the individual requesting access by some unique personal characteristic.*
- *The automated personnel access control system should authenticate an individual's authorization to enter the SCIF by matching the applicable information specified in the previous paragraph with personnel data contained in an automated database to authenticate the individual's authorization prior to giving the individual access to the SCIF.*
- *Automated personnel access control equipment or devices will ensure that the probability of an unauthorized individual gaining access is no more than one in ten thousand while the probability of an authorized individual being rejected access is no more than one in one thousand. Manufacturers will certify in writing that their equipment conforms to this criterion.*
- *Physical security protection will be established and continuously maintained for all devices/equipment that comprise the personnel access control system. The level of protection may vary depending upon the type of devices/equipment being protected. Existing security controls within the facility will be used to the extent practical in meeting this requirement.*
- *The transmission line will be installed within a protective covering to preclude surreptitious manipulation or be adequately supervised to protect against modification and/or substitution of the transmitted signal.*
- *Electric door strikes installed for use in personnel access control systems will be heavy-duty industrial grade.*
- *Locations where authorization data, card encoded data and personal identification or verification data is input, stored, or recorded will be protected within a SCIF or an alarmed area controlled at the SECRET level. Records and information concerning encoded ID data, PINs, authentication data, operating system software, or any identifying data associated with the personnel access control system is kept secured when unattended. Access to the data will be restricted.*
- *Card readers, keypads, communication, or interface devices located outside the entrance to a SCIF will have tamper resistant enclosures and are securely fastened to a wall or other structure.*
- *Electrical components, associated wiring, or mechanical links (e.g., cables, rods, etc.) will be accessible only from inside the SCIF or if they transverse an uncontrolled area they are secured within a protective covering to preclude surreptitious manipulation of components.*
- *Records will be maintained to reflect the current active assignment of ID badge/card, PIN, level of access, entries and similar system-related elements. Records concerning personnel removed from the system will be for a minimum of 2 years. Records of entries to SCIFs will be for a minimum of 2 years or until*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

*investigations of system violations and incidents have been successfully resolved and recorded.*

2. The assessor must verify whether sufficient access control procedures, systems and devices are in place to control admittance to SCIF areas.
- ◆ *It is recommended that non-automated access control (i.e., electric, mechanical, electro-mechanical) that meets the criteria stated below may be used to control admittance to SCIF areas during working hours if the entrance is under visual control. These systems will be acceptable to control access to compartmented areas within the SCIF. Non-automated access system devices will be installed in the following manner:*
    - *It is recommended that the control panel in which the combination and all associated cabling and wiring is set will be located inside the SCIF and requires minimal physical security designed to deny unauthorized access to its mechanism. The control panel will be installed or have a shielding device mounted, such that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.*
    - *It is recommended that keypad devices will be designed or installed in such a manner that unauthorized individuals in the immediate vicinity cannot observe the entry of the access code.*
  - ◆ *It is recommended that operating personnel access control systems requires that the below personnel requirements and restrictions be followed:*
    - *It is recommended that personnel entering or leaving a SCIF will be required to ensure the entrance or exit point is properly closed. Authorized personnel who permit another individual to enter the area are responsible for confirming the individual's access and need-to-know.*
    - *It is recommended that a SCIF indoctrinated person who is knowledgeable of the security procedures of the SCIF will continuously escort persons within the SCIF who are not Sensitive Compartmented Information (SCI) indoctrinated.*
    - *It is recommended that access to records and information concerning encoded ID data and PIN will be restricted to SCI-indoctrinated personnel. Access to identification or authentication data, operating system software, or any identifying data associated with the personnel access control system is limited to the least number of personnel possible.*
    - *It is recommended that SCI-indoctrinated individuals will select and set the combinations for non-automated access controls. The combination will be changed when compromised or an individual knowledgeable of the combination no longer requires access.*
    - *It is recommended that a procedure be established for removing an individual's authorization to enter an area when the individual is transferred, terminated, or*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

*the individual's access is suspended, revoked, or downgraded to a level below that required for entry. Compromised access cards and/or PINs will be immediately reported and removed from the system.*

- *It is recommended that access rosters listing all persons authorized access to the facility will be maintained at the SCIF point of entry. Electronic systems, including coded security identification cards or badges, may be used in lieu of security access rosters.*
- *It is recommended that each SCIF will have procedures for identification and control of visitors seeking access to the SCIF.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PHYSICAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>TRAINING</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Physical Security Training refers to those training programs required to ensure security staff qualifications, meet periodic employee training requirements, promote employee security awareness and ensure that employees are trained as appropriate for their position and level of responsibility.</p>
<p><b><u>INTENT:</u></b> To ensure that security staff personnel are appropriately trained to increase employee security awareness and to instill in personnel a sense of ownership for the security and protection of critical assets. Training will also enable employees to anticipate and recognize potential threats and to react quickly and correctly to threats and undesirable events.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> The assessment of Physical Security Training will include the review of education and training of personnel assigned to the facility. This assessment will include verification that required initial and refresher physical security-related training is provided to military and civilian personnel, verification of instructor’s qualifications and the maintenance of required training records. Additionally, measures taken by the facility’s security staff to remind and educate personnel of threats will be assessed.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Physical Security Training are based on guidelines contained in DoD O-2000.12H: <i>Protection of DoD Personnel and Assets from Acts of Terrorism (dated October 2000)</i>, DTRA Antiterrorism Vulnerability Assessment Team Guidelines (dated October 2001), AFI 31-101: <i>The Air Force Installation Security Program (dated 1 June 2000)</i>, AFI 31-401: <i>Information Security Program Management (dated November 2001)</i> and DoDI 2000.18: <i>Department of Defense Installation Chemical, Biological, Radiological, Nuclear and High Yield Explosive Emergency Response Guidelines (dated 4 December 2002)</i>. These references address the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p>

## For Official Use Only

### Draft CIP FSVA Physical Security Standards

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether security managers have received training designed to equip the appointees with a workable knowledge and understanding of information security, personnel security, and industrial security program mandates, including security access requirements and organizations manpower document position coding.
  - ◆ *It is recommended that security managers receive training within 90 days of their assignment and a record of training will annotated in the individual's official personnel file.*
2. The assessor must verify whether training and awareness programs are addressed in the asset's Physical Security Plan, Continuity of Operations (COOP) Plan and other contingency plans.
  - ◆ *It is recommended that training will include physical awareness training, region specific training, threat briefings, physical security training, and advanced training regarding the protection of critical assets and record keeping.*
3. The assessor must verify whether physical security training is sufficient and conducted annually for personnel working with designated critical assets and records of training will be documented.
  - ◆ *It is recommended that individuals working with critical assets assigned outside the U.S. for either permanent or temporary work assignments complete the prescribed general physical security awareness training and specific regionally focused training. Every critical asset (e.g., facility, site etc.) will have at least one security officer who has completed advanced physical security training. The security officer will be designated in writing.*
  - ◆ *It is recommended that security awareness programs use meetings and available media such as newspapers and intranets to increase awareness. The Physical Security Plan should describe the programs, delineate responsibilities and provides procedures for reporting suspicious activity.*
  - ◆ *It is recommended that all personnel working with critical assets be trained in actions (e.g., delivery inspections, bomb threat procedures, access control, etc.) to implement prescribed random physical security measures required during elevated threat levels.*
  - ◆ *It is recommended that the critical asset staff-training program provide for the necessary initial and periodic refresher training appropriate to the different emergency responsibilities.*
  - ◆ *It is recommended that the critical asset/facility exercise program ensure that exercise base contingency plans are exercised annually.*

**For Official Use Only**  
**Draft CIP FSVA Physical Security Standards**

- ◆ *It is recommended that the scope of drills and exercises test the integrated response capabilities of internal and external supporting emergency organizations.*
- ◆ *It is recommended that training exercises include bomb threat scenarios and building evacuations.*
- ◆ *It is recommended that security managers of critical assets/facilities ensure that supporting Explosive Ordnance Disposal (EOD) response assets are integrated into exercise planning and participate in the integrated response.*
- ◆ *It is recommended that problems or shortcomings identified during drills and exercises be documented, tracked, and tested in future drills in order to ensure that performance deficiencies are corrected. Plans will be updated accordingly.*
- ◆ *It is recommended that basic and advance security training programs be developed at all facilities possessing or supporting protection level resources.*
- ◆ *It is recommended that training of security forces protecting critical assets emphasize individual and collective rehearsal of tactical response skills and plans designed to deny or defeat intrusive threats.*
- ◆ *It is recommended that security forces for critical assets incorporate innovative training aids to provide realistic tactical training.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

**INFORMATION SECURITY**

**DESCRIPTION:**

Information Security is the process of securing critical assets data that are vital to United States (U.S.) National Security through a series of guidelines (e.g., policies, directives, plans, etc.). These guidelines cover how the critical asset's data will be secured in a system and establish how personnel can access the critical data within the system. The end goal of Information Security is to protect critical assets data against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional, while ensuring that the data is available when needed.

<b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i>
<b><u>TOPIC:</u></b> <i>PHYSICAL ACCESS CONTROLS</i>
<b><u>SUBTOPIC:</u></b> <i>RULES OF BEHAVIOR</i>
<b><u>EXPLANATION:</u></b> Rules of Behavior refer to the policies, plans and guidelines that have been established concerning use of, security in and acceptable level of risk for the critical assets. The rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules of behavior will also address the consequences of inconsistent behavior or non-compliance. These rules will be documented in writing and form the basis for security awareness and training with regards to a DoD critical asset.
<b><u>INTENT:</u></b> To ensure that all users understand their responsibilities and expected behavior with regard to access to an information system that has been designated as a critical asset and to ensure that they understand the consequences of behavior that is inconsistent with the established rules.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Rules of Behavior for a critical asset will include a review of polices, plans and guidelines from a Critical Infrastructure Protection (CIP) perspective in the following areas: security plans, physical security, access controls, and password usage.

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

**CRITERIA:**

The standards for the assessment of Rules of Behavior are based on guidelines contained in *Office of Management and Budget (OMB) A-130 (dated 10 November 2003)*, *"The Internal Threat to Security" SANS Institute (dated March 2003)*, *the Rainbow Library Green Book (dated April 1985)*, *National Institute of Standards and Technology (NIST) 800-26: Security Self-Assessment Guide for Information Technology Systems (dated November 2001)*, and *Department of Defense (DoD) 5220.22-M National Industrial Security Program Operating Manual (NISPOM) (dated January 1995), incorporating Change One (dated July 1997) and Change Two (dated February 2001)*. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether adequate information security policies and procedures to inform users, staff, and managers of their obligatory requirements for protecting critical technology and information assets are in place and being exercised.
  - ◆ *It is recommended that these policies specify the mechanisms through which these requirements can be met. An organization's Information Security Policy should address the following items:*
    - *An Access Policy that defines access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management. It will provide guidelines for external connections, data communications, connecting devices to a network and adding new software to systems. It will also specify any required notification messages.*
    - *An Accountability Policy that defines the responsibilities of users, operations staff, and management. It will specify an audit capability and provide incident handling guidelines.*
    - *An Authentication Policy that establishes trust through an effective password policy and by setting guidelines for remote location authentication and the use of authentication devices.*
    - *An Availability Statement that sets users' expectations for the availability of resources. It will address redundancy and recovery issues as well as specify operating hours and maintenance downtime periods. It will also include contact information for reporting system and network failures.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- *An Information Technology System and Network Maintenance Policy that describes how both internal and external maintenance people are allowed to handle and access technology. One important topic is whether remote maintenance is allowed and how such access will be controlled.*
  - *A Violations Reporting Policy that indicates types of violations (e.g., privacy and security, internal and external, etc.) that will be reported and to whom the reports are made.*
  - *A Training Policy that describes the required training and frequency of training.*
  - *Supporting information that provides users, staff and management with contact information for each type of policy violation, guidelines on how to handle outside queries about a security incident or information that may be considered confidential or proprietary and cross-references to security procedures and related information such as company policies and governmental laws and regulations.*
2. The assessor must verify whether adequate information security plans are developed and being exercised.
- ◆ *It is recommended that the following information security plans are developed:*
  - ◆ *The system security plan should be consistent with guidance issued by the NIST. Independent advice and comment on the security plan will be solicited prior to the plan's implementation. System Security plans for critical assets will include the following:*
    - *Establish a set of rules of behavior concerning system use, system security and the acceptable level of risk.*
    - *Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system.*
    - *Screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening will occur prior to an individual being authorized to bypass controls and periodically thereafter.*
    - *Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.*
    - *Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.*
    - *Ensure that cost-effective security products and techniques will be appropriately used within the system.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- *Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. Where connection is authorized, controls will be established that are consistent with the rules of the system and in accordance with guidance from NIST.*
3. The assessor must verify whether adequate network security plans have been developed and are exercised.
- ◆ *It is recommended that every network have a network security plan. Specific network requirements should be determined on a case-by-case basis. The security plan for the network should address the following additional requirements:*
    - *Description of security services and mechanisms protecting against network specific threats.*
    - *Consistent with its mode of operation, the network will provide the following security services:*
      - *Access Control*
      - *Data Flow Control*
      - *Data Separation*
      - *Auditing*
      - *Communications Integrity*
    - *Consistent implementation of security features across the network components.*
    - *Configuration control of network interconnections.*
    - *Protection and control of data transfers.*
    - *Security features incorporated in communications protocols.*
    - *Adequacy of any filtering bridge, secure gateway or other similar security device in controlling access and data flow.*
    - *Compatibility of the entire combination of operating modes when connecting a new system.*
    - *Adequacy of the external system's features to support the local security policy.*
4. The assessor must verify whether adequate application security plans have been developed and are exercised.
- ◆ *It is recommended that this plan will be consistent with guidance issued by NIST and OMB Circular A-130. The plans will include the following areas:*
    - *A set of rules concerning use of and behavior within the application will be established.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- *Ensure that all individuals receive specialized training, focused on their responsibilities and the application rules, before permitting them access to the application.*
  - *Incorporate controls such as separation of duties, least privilege and individual accountability into the application and application rules as appropriate.*
  - *Establish and periodically test the capability to perform the organization's function supported by the application in the event of failure of its automated support.*
  - *Ensure that appropriate security controls are specified, designed into, tested and accepted in the application in accordance with appropriate guidance issued by NIST.*
  - *Ensure that information shared from the application is protected appropriately, comparable to the protection provided when information is within the application.*
  - *Where an organizations application promotes or permits public access, additional security controls should be added to protect the integrity of the application. Controls should include segregating information made directly accessible to the public from official organizational records.*
5. The assessor must verify whether adequate physical security measures are in place to prevent unauthorized access to information.
- ◆ *It is recommended that all remote network equipment be placed in wiring closets. These closets will be locked with either a cipher lock or a key that is controlled or a locked network rack.*
  - ◆ *It is recommended that all network cabling be run in the ceiling, walls, or under raised floors. Wire should never be taped to the floor in accessible locations. Patch cabling run along the outside of walls should be attached to the baseboard.*
  - ◆ *It is recommended that all wiring and port assignments be properly identified and noted on a schematic diagram. This network mapping will be maintained and updated any time the network is modified. This solution will help ensure network drops remain where they are placed and will also assist in planning for future growth and troubleshooting issues.*
  - ◆ *It is recommended that physical security safeguards be established that prevent or detect unauthorized access to accredited system entry points and unauthorized modification of the Automated Information System (AIS) hardware and software. Hardware integrity of the AIS, including remote equipment, be maintained at all times, even when the AIS is not processing or storing classified information.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- ◆ *It is recommended that attended classified processing should take place in an area, normally a Restricted Area, where authorized persons can exercise constant surveillance and control of the AIS. All unescorted personnel to the area have a government granted security clearance and controls should be in place to restrict visual and aural access to classified information.*
  - ◆ *It is recommended that when the AIS is not in use, all classified information has been removed and properly secured and the AIS has been downgraded. Continuous physical protection should be implemented through one or more of the following methods:*
    - *Continuous supervision by authorized personnel.*
    - *Use of approved cabinets, enclosures, seals, locks or closed areas.*
6. The assessor must verify whether sufficient physical security controls have been implemented to restrict physical access to critical assets and protect them from intentional/unintentional loss or impairment.
- ◆ *It is recommended that these resources include the following:*
    - *Primary computer facilities*
    - *Cooling system facilities*
    - *Terminals that are used to access a computer*
    - *Microcomputers/Computer file storage areas*
    - *Telecommunications equipment and lines, including wiring cabinets*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i>
<b><u>TOPIC:</u></b> <i>PHYSICAL ACCESS CONTROLS</i>
<b><u>SUBTOPIC:</u></b> <i>AUDITING</i>
<b><u>EXPLANATION:</u></b> Auditing refers to an electronic or paper log used to track all computer activity and indicate attempts to gain unauthorized access.
<b><u>INTENT:</u></b> To ensure that all auditing mechanisms for critical assets are reviewed regularly in order to detect improper activity or unauthorized access on critical assets.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Auditing of critical assets will include a review of the procedures for recording, analyzing and storage of audit logs.
<b><u>CRITERIA:</u></b> The standards for the assessment of Auditing are based on guidelines contained in <i>"The Internal Threat to Security"</i> SANS Institute (dated March 2003), NIST 800-26: <i>Security Self-Assessment Guide for Information Technology Systems</i> (November 2001), <i>Common Criteria Controlled Access Protection Profile – NSA</i> (undated), DODI 8500.2: <i>IA Program Implementation</i> (dated 6 February 2003), and the NISPOM (dated January 1995), incorporating <i>Change One</i> (dated July 1997) and <i>Change Two</i> (dated February 2001). The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.  In support of a given mission and where applicable, the FSIVA assessor must verify the following:  <ol style="list-style-type: none"><li>1. The assessor must verify whether an auditing policy is in place to track events, file access attempts and record incident data.</li><li>2. The assessor must verify whether audit procedures for records are being followed appropriately to indicate inappropriate or unusual usage.<ul style="list-style-type: none"><li>◆ <i>It is recommended that audit records be protected from unauthorized access, deletion or modification by weekly back up and off site storage.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

3. The assessor must verify whether security audits of classified information systems that are designated as critical assets are sufficient to ensure information security.
- ◆ *It is recommended that regardless of mode of operation, the security logs will include the date, the event, the person responsible, component involved, action taken, installation and the software involved, the testing, modification of operating system and security related software, maintenance, repair, installation or removal of hardware component.*
  - ◆ *It is recommended that audit logs will be reviewed and analyzed at specified intervals.*
  - ◆ *It is recommended that the system will create an audit trail of auditable events: date and time of the event, type of event, successful and unsuccessful login attempts, password changing and origin of the event.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>DATA STORAGE, CONTROL, AND ACCESS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>RECORDS MANAGEMENT</i></p>
<p><b><u>EXPLANATION:</u></b> Records Management refers to how and where critical asset data is stored and controlled and who is permitted to access the data.</p>
<p><b><u>INTENT:</u></b> To ensure that access to stored critical asset data is protected from unauthorized users and to restrict access to data to only users who are in need of the information.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Records Management for a critical asset will include a review of media controls, software controls, access controls and operating systems guidelines.</p>
<p><b><u>CRITERIA:</u></b> The standards and recommendations for the assessment of Records Management are based on guidelines contained in <i>DoDI 8500.2: IA Program Implementation (dated 6 February 2003)</i>, the <i>NISPOM (dated January 1995)</i>, incorporating <i>Change One (dated July 1997)</i> and <i>Change Two (dated February 2001)</i>, the <i>Rainbow Library Green Book</i> and from the <i>SANS Institute</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether media control procedures are being sufficiently addressed and exercised to ensure information security.<ul style="list-style-type: none"><li>◆ <i>It is recommended that all data storage media for compartmented and multilevel AIS will be labeled and controlled to the highest level of the information contained on the media.</i></li><li>◆ <i>It is recommended that storage media be sanitized and declassified prior to release from continuous protection.</i></li></ul></li><li>2. The assessor must verify whether software control procedures are being sufficiently addressed and exercised to insure information security.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- ◆ *It is recommended that the security policy provide procedures for approval of installation of any software on the AIS.*
  - ◆ *It is recommended that contractor personnel that design, develop, test, install or make modifications to systems or use security software be cleared to the level of the AIS.*
  - ◆ *It is recommended that incidents involving malicious software be investigated immediately. If the incident affects the integrity of classified information, the security officer will be notified immediately and a written report detailing the findings of this investigation will be submitted in accordance with the security policy.*
3. The assessor must verify whether access control procedures are being sufficiently addressed and exercised to ensure information security.
- ◆ *It is recommended that access controls be established.*
  - ◆ *It is recommended that separation of duties between security personnel who administer the access control function and those who administer the audit trail be implemented.*
  - ◆ *It is recommended that physical and logical access controls be established to enforce the segregation of duties.*
  - ◆ *It is recommended that system password policies be defined so that all user accounts are protected with strong passwords. The following are recommendations regarding password protection:*
    - *“Out of the box “ passwords and user IDs will be changed (e.g., vendor user IDs such as SYSTEM, ADMIN, etc.).*
    - *System administrators will be notified when a user has forgotten the password or the password may have been compromised or when a user ID and password will be removed from the system (e.g., when an employee leaves the sponsoring organization, etc.).*
    - *Passwords will have a set maximum lifetime.*
4. The assessor must verify whether user interface services are physically or logically separated from data storage and management.
- ◆ *It is recommended that this separation be accomplished through the use of different computers, different Central Processing Units (CPUs), different instances of the operating system, different network addresses, or a combination of methods as appropriate.*
5. The assessor must verify whether the following adequate procedures are being followed when providing information to the Internet Domain Naming Service (DNS).

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- ◆ *It is recommended that position titles be listed rather than staff names.*
- ◆ *It is recommended that an 800 phone number be used to guard against war dialing.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>DATA STORAGE, CONTROL, AND ACCESS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>BACKUP ON-SITE</i></p>
<p><b><u>EXPLANATION:</u></b> Backup On-Site refers to the procedures and policies dealing with periodic backup of a critical asset and storage of that data in the same vicinity as the information system.</p>
<p><b><u>INTENT:</u></b> To ensure a backup is conducted so that restoration of an information system that is designated as a critical asset is possible.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of critical asset Backup On-Site will include a review of service continuity and contingency plans.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Backup On-Site are based on guidelines contained in <i>DODI 8500.2: IA Program Implementation (dated 6 February 2003)</i>, <i>NIST 800-26: Security Self-Assessment Guide for Information Technology Systems (dated November 2001)</i> and <i>Federal Information Systems Controls Audit Manual (FISCAM) (undated)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether procedures are in place to assure the physical and technical protection of the backup and restoration hardware, firmware and software.</li><li>2. The assessor must verify whether backups of the operating system and other critical software are stored in a fire rated container or are located separately from operational software.</li><li>3. The assessor must verify whether recovery procedures and technical system features ensure that recovery is performed in a secure and verifiable manner.</li><li>4. The assessor must verify whether critical data files and operations have been identified and documented.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

5. The assessor must verify whether Service Continuity procedures are in place to sufficiently protect information resources.
- ◆ *It is recommended that procedures be in place to protect information resources and minimize the risk of unplanned interruptions as well as a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities as well as the activities performed by users of specific applications.*
  - ◆ *It is recommended that recovery plans be tested periodically in disaster simulation exercises.*
  - ◆ *It is recommended that the minimum resources required to support critical data and operations be identified and their role analyzed. The resources to be considered include computer resources such as computer hardware, software and data files, telecommunications services and other resources that are necessary to the operation.*
  - ◆ *It is recommended that a plan for restoring critical operations be implemented. The plan should clearly identify the order in which various processing will be restored, who is responsible and what supporting equipment or other resources will be required.*
6. The assessor must verify whether a contingency plan has been developed, communicated to affected staff and updated periodically to reflect current operations.
- ◆ *It is recommended that this plan provide information on required supporting resources, key roles and responsibilities, arrangements for alternate site disaster recovery operations and procedures for restoring critical applications and their order in the restoration process.*
  - ◆ *It is recommended that multiple copies of the contingency plan be available, with some stored at alternate locations, to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>DATA STORAGE, CONTROL, AND ACCESS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>ALTERNATE SITE</i></p>
<p><b><u>EXPLANATION:</u></b> Alternate Site refers to the procedures and policies dealing with periodic backup and storage of critical asset data in a separate geographical area from the information system.</p>
<p><b><u>INTENT:</u></b> To ensure backup of critical asset data is conducted so that continuity of operations plans can be instituted in the case that the original critical asset is not operational and cannot be restored.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Alternate Site for a critical asset will include a review of contingency plans, backup plans and guidelines.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Alternate Site are based on guidelines contained in <i>DODI 8500.2: IA Program Implementation (dated 6 February 2003)</i> and <i>NIST 800-26: Security Self-Assessment Guide for Information Technology Systems (dated November 2001)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether a contingency plan provides a smooth transfer of all mission and business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity.<ul style="list-style-type: none"><li>◆ <i>It is recommended that the alternate site will provide security measures equivalent to the primary site.</i></li><li>◆ <i>The assessor must verify whether data backup for the primary site is accomplished by maintaining a redundant secondary system at the alternate site that can be activated without loss of data or disruption to the operation.</i></li><li>◆ <i>It is recommended that backup files be created on a prescribed basis and stored at the alternate site.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i>
<b><u>TOPIC:</u></b> <i>NETWORK SYSTEMS</i>
<b><u>SUBTOPIC:</u></b> <i>MAINTENANCE</i>
<b><u>EXPLANATION:</u></b> Maintenance of Network Systems designated as critical assets refers to the daily processes and procedures used to sustain the network and keep it in optimum operational condition.
<b><u>INTENT:</u></b> To sustain a critical operational network by minimizing risks of any threats and to reduce the risks of a critical system disruption by ensuring that effective critical asset network system maintenance programs and practices are in place.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Maintenance Network Systems will include a review of maintenance support, plans, procedures and personnel.
<b><u>CRITERIA:</u></b> The standards for the assessment of Maintenance of Network Systems are based on guidelines contained in <i>DODI 8500.2: IA Program Implementation (dated 6 February 2003)</i> , <i>NIST 800-26: Security Self-Assessment Guide for Information Technology Systems (dated November 2001)</i> and the <i>NISPOM (dated January 1995)</i> , incorporating <i>Change One (dated July 1997)</i> and <i>Change Two (dated February 2001)</i> . The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.  In support of a given mission and where applicable, the FSIVA assessor must verify the following:  1. The assessor must verify whether maintenance support and procedures are sufficient to sustain a critical operational network by minimizing risks of any threats and to reduce the risks of a critical system disruption by ensuring that effective critical asset network system maintenance programs and practices are in place.  ◆ <i>It is recommended that maintenance support and spare parts be available 24X7 upon failure.</i>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

2. The assessor must verify whether data backup for the primary site is accomplished by maintaining a redundant secondary system at the alternate site that can be activated without loss of data or disruption to the operation.
- ◆ *It is recommended that cleared personnel when possible, perform maintenance and repair activities. If uncleared personnel will be performing maintenance, steps should be taken to effectively deny access to classified information. A cleared and technically knowledgeable individual should always escort uncleared maintenance personnel. These procedures should be documented in the security policy.*
  - ◆ *It is recommended that uncleared personnel not use the dedicated copy of the system software with a direct security function for maintenance purposes.*
  - ◆ *It is recommended that all maintenance and diagnostics be performed in the contractor facility. Any AIS components or equipment released from secure control should no longer be a part of an accredited system.*
  - ◆ *It is recommended that remote diagnostic or maintenance services be strongly discouraged. If remote diagnostic or maintenance services become necessary, the AIS should be sanitized and disconnected from any communication links to networks prior to the connection of any non-secured communication line.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i>
<b><u>TOPIC:</u></b> <i>NETWORK SYSTEMS</i>
<b><u>SUBTOPIC:</u></b> <i>INTRUSION DETECTION SYSTEM AND NETWORK BOUNDARY CONTROL</i>
<b><u>EXPLANATION:</u></b> Intrusion Detection System (IDS) is a type of security management system for computers and networks that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. Among other tools an IDS can be used to determine if a computer network or server has experienced an unauthorized intrusion. Network Boundary Control is comprised of software (i.e., firewall, protocols, services, etc.) hardware (i.e., firewall, routers, bridges, Network Device Controls, etc.) and services. Network Boundary Control protects computers and networks from external security breaches. Among other tools firewalls can be used to determine if a computer network or server has experienced an unauthorized intrusion.
<b><u>INTENT:</u></b> To detect inappropriate, incorrect, or anomalous activity to prevent access to the critical asset by unauthorized users.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of IDS and Network Boundary Control will include at a review of the following areas: Firewall Policy, Ports, Protocols, and Services, and Network Device Controls. Intrusion detection functions include: monitoring and analyzing both user and system activities, analyzing system configurations and vulnerabilities, assessing system and file integrity, recognizing patterns of typical attacks, analysis of abnormal activity patterns and tracking user policy violations.
<b><u>CRITERIA:</u></b> The standards for the assessment of IDS and Network Boundary Control are based on guidelines contained in <i>NIST SP 800-41: Guidelines on Firewalls and Firewall Policy (dated January 2002)</i> , <i>DoDI 8500.2: IA Program Implementation (dated 6 February 2003)</i> and <i>NIST 800-26: Security Self-Assessment Guide for Information Technology Systems (dated November 2001)</i> . The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether firewall policy has been developed and implemented in accordance with *NIST SP 800-41*.
2. The assessor must verify whether a sufficient network device control program (e.g., routers, switches, firewalls, etc.) has been implemented.
  - ◆ *It is recommended that this program include the following:*
    - *Instructions for restart and recovery procedures*
    - *Restrictions on source code access, system utility access and system documentation*
    - *Protection from deletion of system and application files*
    - *A structured process for implementation of directed solutions (e.g., the DoD Information Assurance Vulnerability Alert (IAVA), etc.)*
    - *Audit or other technical measures will be in place to ensure that the network device controls are not compromised. Change controls should be periodically tested.*
    - *Boundary defense mechanisms to include firewalls and IDS should be deployed at the enclave boundary.*
    - *Both inbound and outbound instant messaging should be blocked at the enclave boundary unless the messaging services are configured by an application or enclave to perform an official and authorized function.*
    - *Penetration testing should be performed on the system.*
    - *Communication with Computer Emergency Response Team/Command Center (CERT/CC) and Federal Computer Emergency Response Team/Command Center (FEDCERT/CC) should be on a routine basis in order to provide early warning detection and protection.*
3. In the context of interconnections, the assessor must verify the following:
  - a. The assessor must verify whether the hardware, software, and firmware required to adjudicate security policy and implementation differences between and among connecting classified information systems that are a part of the Security Support Structure (SSS) are accredited.
    - ◆ *It is recommended that the following requirements be satisfied as part of the SSS accreditation:*
      - *Document the security policy enforced by the SSS.*
      - *Identify a single mode of operation.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- *Document the network security architecture and design.*
  - *Document minimum contents of memorandums of agreement (MOAs) required for connection to the SSS.*
  - b. The assessor must verify whether separately accredited network (SAN) is a medium of interconnection of convenience and if networks and/or AISs that are interconnected through a SAN meet the connection rules of the SAN.
  - c. The assessor must verify whether the interconnection of previously accredited systems into an accredited network requires a re-examination of the security features and assurances of the contributing systems to ensure their accreditations remain valid.
  - d. The assessor must verify whether an interconnected network is defined and accredited, and if additional networks and separately accredited AISs are connected through the accredited SSS.
  - e. The assessor must verify whether the addition of components to contributing unified networks that are members of an accredited interconnected network are allowed, provided these additions do not change the accreditation of the contributing system.
4. The assessor must verify whether Protected Distribution Systems or National Security Agency approved encryption methodologies and devices are used to protect classified information when it is being transmitted between network components.

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>NETWORK SYSTEMS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>INTERNAL NETWORK SECURITY</i></p>
<p><b><u>EXPLANATION:</u></b> Internal Network Security refers to the practice of evaluating and monitoring the internal information processing environment, and protecting the network from users who already have access, as opposed to focusing on threats from outside the network. These functions include monitoring and analyzing both user and system activities, analyzing system configurations and vulnerabilities, assessing system and file integrity, ability to recognize patterns of typical insider attacks, analysis of abnormal activity patterns and tracking user policy violations.</p>
<p><b><u>INTENT:</u></b> To detect inappropriate, incorrect or anomalous activity on critical assets in order to prevent authorized users from harming the network or computer.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of critical asset Internal Network Security will include a review of web browsing, IDS and privileged account management.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Internal Network Security are based on guidelines contained in <i>DODI 8500.2: IA Program Implementation (dated 6 February 2003)</i> and from the <i>SANS Institute</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic. In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether web surfing capabilities are limited to only those that are necessary.</li><li>2. The assessor must verify whether host based IDS is deployed for major applications and for network management assets.</li><li>3. The assessor must verify whether all privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration, etc.).</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i>
<b><u>TOPIC:</u></b> <i>NETWORK SYSTEMS</i>
<b><u>SUBTOPIC:</u></b> <i>MALICIOUS CODE</i>
<b><u>EXPLANATION:</u></b> Malicious Code refers to various types of software that can cause problems or damage a computer or network. The more common classes of programs referred to as malicious code are viruses, worms, trojan horses, macro viruses and backdoors.
<b><u>INTENT:</u></b> To prevent disruption to critical assets due to the introduction of malicious code.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Malicious Code will include a review of anti-viral software and updates.
<b><u>CRITERIA:</u></b> The standards for the assessment of Malicious Code are based on guidelines contained in <i>DODI 8500.2: IA Program Implementation (dated 6 February 2003)</i> , <i>NIST 800-26: Security Self-Assessment Guide for Information Technology Systems (dated November 2001)</i> and from the <i>SANS Institute</i> . The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.  In support of a given mission and where applicable, the FSIVA assessor must verify the following: <ol style="list-style-type: none"><li>1. The assessor must verify whether all servers, workstations, and mobile computing devices implement virus protection that includes a capability for automatic updates.</li><li>2. The assessor must verify whether a properly implemented anti-viral plan includes automated virus warnings from vendors and a daily review of vendor cites for new virus definition files and information.</li><li>3. The assessor must verify whether Virus Detection and elimination software is installed and updated regularly.<ul style="list-style-type: none"><li>◆ <i>It is recommended that virus scanning be automatic and all servers and workstations will be routinely scanned for viruses.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- ◆ *It is recommended that random checks of workstations be used to ensure they are being scanned and updated.*
- ◆ *It is recommended that mail servers automatically delete or quarantine suspicious files and forward a message to the recipient or sender.*
- ◆ *It is recommended that policies be put in place to ensure that workstations are configured to prevent the download and execution of executable mobile code.*

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>NETWORK SYSTEMS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>ENVIRONMENTAL CONTROLS</i></p>
<p><b><u>EXPLANATION:</u></b> Environmental Controls refers to the measures and procedures used to reduce the possibility of damage to a critical asset information system or its components that may be caused by environmental conditions or hazards.</p>
<p><b><u>INTENT:</u></b> To prevent unavailability of a critical asset information system because of environmental hazards or conditions.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Environmental Controls of a critical asset information system will address a review of the emergency lighting, fire emergency systems, heating and air conditioning and power distribution systems and other utilities.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Environmental Controls will be based on guidelines contained in <i>DODI 8500.2: IA Program Implementation (dated 6 February 2003)</i> and <i>NIST 800-26: Security Self-Assessment Guide for Information Technology Systems (dated November 2001)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic. In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether emergency lighting has been installed to cover all areas necessary to maintain mission or business essential functions, as well as emergency exits and evacuation routes.</li><li>2. The assessor must verify whether stand-alone fire/smoke detectors have been properly installed and maintained.</li><li>3. The assessor must verify whether periodic fire marshal inspections occur.</li><li>4. The assessor must verify whether a servicing fire department receives an automatic notification of any activation of fire suppression system or smoke alarm.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

5. The assessor must verify whether automatic temperature and humidity controls are in place to prevent fluctuations potentially harmful to the equipment.
  - ◆ *It is recommended that a redundant air-cooling system be in place.*
6. The assessor must verify whether an automatic voltage control is implemented and electrical systems are configured to allow continuous or uninterrupted power.

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>INFORMATION SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>TRAINING</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>END-USER AND SYSTEM STAFF TRAINING</i></p>
<p><b><u>EXPLANATION:</u></b> End User and System Staff Training refers to initial and ongoing training that staff members and end users receive.</p>
<p><b><u>INTENT:</u></b> To ensure that the end users and IT staff members understand and acknowledge the security policies and procedures of a critical asset. Additionally, to ensure that the IT staff remains current on new technologies and developments in their areas of expertise.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of End User Training will include a review of the training materials that are used as well as spot checks of personnel to ensure that they received the training prior to gaining access to the system, as well as follow-up training. An assessment of System Staff Training will include a review of the End User Initial Training materials, as well as the staff training materials. It will also include a review of courses that are offered to IT staff, as well as courses that have been taken previously.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of End User and System Staff Training are based on guidelines contained in <i>NIST 800-26: Security Self-Assessment Guide for Information Technology Systems (dated November 2001)</i>, and the <i>Rainbow Library Green Book (undated)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic. In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether adequate information security training is established and provided to all end users prior to gaining access to the information system.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Information Security Standards**

- ◆ *It is recommended that all end users receive initial information security training before gaining access to the information system and periodic refresher training thereafter.*
- ◆ *It is recommended that this training include an explanation of the security policies and procedures, an explanation of the current security threats and cautions, as well as basic security Do's and Don'ts. Periodic refresher training emphasizes changes to the operational condition and the threat environment.*
- ◆ *It is recommended that the System Staff Initial Training, as well as the End User Initial Training, be conducted before gaining access to the information system. It should be tailored to the staff and their roles where applicable and will consist of the following:*
  - *Why information security is important to the organization.*
  - *What the organization's information security policy is.*
  - *What procedures the staff is expected to follow.*
- ◆ *It is recommended that opportunities for additional coursework be offered to all system staff to increase their knowledge and proficiency and on the job training will be conducted daily, as new vulnerabilities arise.*

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

**PERSONNEL/INDUSTRIAL SECURITY**

**DESCRIPTION:**

Personnel/Industrial Security involves the use of safeguards, including clearances, credentials, training, and document control and accountability, necessary to prevent the unauthorized access to a critical asset or unauthorized disclosure of classified information pertaining to a critical asset. It also involves control of access to critical assets and/or authorized disclosure of classified information pertaining to critical assets released by the United States (U.S.) Government Executive Branch Departments and Agencies to their contractors and to protect special classes of classified information associated with critical assets.

<b><u>AREA OF CONCERN:</u></b> <i>PERSONNEL/INDUSTRIAL SECURITY</i>
<b><u>TOPIC:</u></b> <i>CLEARANCES</i>
<b><u>SUBTOPIC:</u></b> <i>CONTRACTORS AND SERVICE PROVIDERS</i>
<b><u>EXPLANATION:</u></b> Personnel and Industrial Security Clearances refers to Facility Clearances (FCL), which determine that a contractor facility that directly supports a critical asset or houses classified information that is associated with the critical asset is eligible for access to classified information or award of a classified contract. It also refers to Personnel Clearances (PCL) that determine contractor and/or service provider personnel will be declared eligible for access to the critical asset or its classified information at a level identified by the personnel clearance.
<b><u>INTENT:</u></b> To ensure that critical assets and classified information pertaining to those critical assets will be protected from unauthorized disclosure by limiting access to classified information to only those contractor and service provider personnel and contractor facilities that have been determined eligible for access by the clearance determination procedure.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Personnel/Industrial Security Clearances will include a review of all contractor and service provider personnel and contractor facilities currently supporting the critical asset to ensure that only those contractor and service provider

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

personnel and facilities possessing valid clearances have access to critical assets and classified information associated with those assets. Additionally, an assessment will be performed on existing clearance practices and procedures within the critical asset to ensure compliance with the clearance requirements stated in *DoD 5520.22-M National Industrial Security Program Operating Manual (NISPOM) (dated 1995), incorporating Change One (dated July 1997) and Change Two (dated February 2001)*. Finally, an assessment will be performed to determine if background checks are conducted by contract service provider firms for their employees requiring access to critical assets and associated classified information (e.g., cleaning teams, routine maintenance and supply personnel, etc.) and if the asset managers are informed of the results of these background checks.

**CRITERIA:**

The standards for the assessment of Personnel/Industrial Security Clearances for Federal and Contractor Personnel are based on the *NISPOM (dated January 1995), incorporating Change One (dated July 1997) and Change Two (dated February 2001)*. The applicable portions of the above listed reference are listed below and collectively address the required areas for assessment of this subtopic.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether interim FCLs are granted by the Cognizant Security Agency (CSA).
2. The assessor must verify whether procedures for the appropriate level, number and granting of PCLs are granted in a sufficient manner and are consistent with each FCL level.
  - ◆ *It is recommended that contractor firms limit PCLs to the minimum number of employees required for operational efficiency, consistent with the contractual obligations.*
  - ◆ *It is recommended that PCLs of respective levels (e.g., CONFIDENTIAL, SECRET, etc.) be supported by the specific investigative requirements stated in the NISPOM, Chapter 2.*
  - ◆ *It is recommended that non-U.S. citizens are not be granted PCLs; non-U.S. citizens requiring access to classified information relating to critical assets for compelling reasons will be granted Limited Access Authorizations (LAA) only on a case-by-case basis.*
  - ◆ *It is recommended that employees of contract service providers that support facilities housing critical assets (e.g., cleaning teams, maintenance or delivery personnel, etc.) will be vetted by their employers through the conduct of background checks, including law enforcement checks of the national criminal database.*

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PERSONNEL/INDUSTRIAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>CLEARANCES</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>FEDERAL EMPLOYEES</i></p>
<p><b><u>EXPLANATION:</u></b> Personnel and Industrial Security Clearances for Federal Employees refers to the background investigation and clearance of employees for authorizing access to a critical asset or classified information pertaining to the critical asset to a level identified by the personnel clearance.</p>
<p><b><u>INTENT:</u></b> To ensure that critical assets and classified information pertaining to the critical asset are protected from unauthorized disclosure by limiting access to classified information to only those employees of the Federal government that have been determined eligible for access by the clearance determination procedure.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Industrial Security Clearances for Federal Employees will include a review of those federal employees possessing valid clearances with access to critical assets and classified information pertaining to the critical asset. In addition, an assessment of clearances for Federal employees will determine that the eligibility of persons for access to the critical asset or its associated classified information is clearly consistent with the interest of national security.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Personnel/Industrial security clearances for Federal employees are based on guidelines contained in <i>Department of Defense Directive (DoDD) 5200.2: DoD Personnel Security Program (dated 9 April 1999)</i> and <i>Executive Order 12968: Access to Classified Information (dated 2 August 1995)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether procedures for the granting clearances to Federal employees who are granted access to classified information pertaining to a critical asset are sufficient to ensure that information is protected.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

- ◆ *It is recommended that all Federal employees will be subject to a personal security investigation by an appropriate government agency prior to being granted access to classified information pertaining to a critical asset.*
- ◆ *It is recommended that individuals granted security clearances will be briefed prior to being authorized access to classified information and debriefed, as required.*
- ◆ *It is recommended that positions requiring access to critical assets and its associated classified information that are occupied by individuals granted security clearances be periodically reviewed to determine a continuing requirement for access and the associated clearance. When it is determined that access to critical assets and associated classified information is no longer required of a position, clearances should be administratively withdrawn or downgraded.*
- ◆ *It is recommended that employees who are granted eligibility for access to critical assets and related classified information be held responsible for protecting classified information in their custody from unauthorized disclosure, reporting to the security officer all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information.*
- ◆ *It is recommended that employees granted access to critical assets and associated classified information be required, as a condition of access to the asset's classified information, to provide to the employing agency written consent permitting access by an authorized investigative agency to relevant financial records that are maintained by a financial institution (defined in 31 United States Code (U.S.C.) 5312(a)), consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681(a)), and records maintained by commercial entities within the U.S. pertaining to any travel by the employee outside the U.S.*
- ◆ *It is recommended that the head of each agency that grants access to a critical asset and its classified information establish a program for employees with access to classified information to educate employees about individual responsibilities and to inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to the critical asset and associated classified information.*

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

<b><u>AREA OF CONCERN:</u></b> <i>PERSONNEL/INDUSTRIAL SECURITY</i>
<b><u>TOPIC:</u></b> <i>CREDENTIALS</i>
<b><u>SUBTOPIC:</u></b> <i>N/A</i>
<b><u>EXPLANATION:</u></b> Personnel and Industrial Security Credentials refers to the use of a system of passes/badges as a means to verify the bona fides of individuals seeking access to a critical asset or compartmented areas in which classified or sensitive information associated with the critical asset is used and or maintained.
<b><u>INTENT:</u></b> To ensure that only cleared individuals with an established need are granted access to critical asset facilities or compartmented areas where classified or sensitive information is used or maintained.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Personnel/Industrial Security Credentials pertaining to critical assets and classified information related to those assets will include a review of the policies, procedures and practices regarding the use of identification badges, exchange passes and visitor badges. Assessment teams will verify that a pass and badge identification system is in place and used to protect critical assets and related classified information. The assessment will include a review of the procedures to issue, safeguard, account for, recover and dispose of identification badges as required.
<b><u>CRITERIA:</u></b> The standards for the assessment of Personnel/Industrial Security Credentials are based on guidelines contained in <i>DoD O-2000.12-H: Protection of DoD Personnel and Assets from Acts of Terrorism (Draft) (dated October 2000)</i> , <i>DoD 5200.8-R: Physical Security Program (dated May 1991)</i> and <i>Army Regulation (AR) 190-13: The Army Physical Security Program (dated 30 September 1993)</i> . The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this topic.  In support of a given mission and where applicable, the FSIVA assessor must verify the following:  1. The assessor must verify whether the responsible authority has established general procedures for the issue, turn-in, recovery and expiration of security identification cards and badges that permit access to critical assets.

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

- ◆ *It is recommended that blank badges and associated material used in producing badges be secured and accounted for by a designated responsible individual.*
- ◆ *It is recommended that lost or unaccounted for security identification badges be reported and invalidated promptly.*
- ◆ *It is recommended that information displayed on access badges not include the bearer's home address, specific work location address, telephone number and security clearance.*
- ◆ *It is recommended that information identifying the bearer as a DoD or U.S. Government employee not be printed on the badge.*
- ◆ *It is recommended that contractor ID badges be distinguishable from employee badges and will be issued, controlled and accounted for in accordance with the requirements of these standards.*
- ◆ *It is recommended that visitor badges clearly indicate if the visitor requires escort or is eligible for unescorted access.*
- ◆ *It is recommended that visitor badges be inventoried and accounted for daily if self-expiring badges are not used.*

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PERSONNEL/INDUSTRIAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>TRAINING</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Personnel and Industrial Security Training refers to the requirements placed upon contractor firms to provide contractor employees with security training and briefings commensurate with the employees' involvement with critical assets or classified information pertaining to critical assets.</p>
<p><b><u>INTENT:</u></b> To ensure that all contractor support personnel requiring access to critical assets or involved in handling and using classified information, including Facility Security Officers (FSOs) or cleared employees providing only temporary help, receive all appropriate initial training, refresher training, and debriefings as prescribed in the <i>NISPOM, Chapter 3</i>.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment will include a review of training schedules and training records to determine whether or not cleared personnel requiring access to critical assets and associated classified information have received or are scheduled to receive initial security briefs and refresher training as prescribed by of the <i>NISPOM, Chapter 3</i>.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Personnel/Industrial Training are based on guidelines contained in the <i>NISPOM (dated January 1995), incorporating Change One (dated July 1997) and Change Two (dated February 2001) and Army Field Manual 24-17: Tactical Records Traffic System (dated 17 September 1991)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this topic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether or not cleared personnel requiring access to critical assets and associated classified information have received or are scheduled to receive initial security briefs and refresher training as prescribed by of the <i>NISPOM, Chapter 3</i>.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

- ◆ *It is recommended that initial security briefings be provided to appropriate employees prior to being granted access to the critical asset or classified information pertaining to the critical asset.*
- ◆ *It is recommended that Initial security briefings include information regarding potential threats that seek to compromise critical assets or associated classified information, including local and regional criminal and terrorist threats.*
- ◆ *It is recommended that personnel granted access to critical assets and classified information related to the asset receive refresher security training annually.*
- ◆ *It is recommended that refresher training inform employees of changes to critical asset security regulations and requirements as well as changes to the threat environment as it pertains to the control and protection of the asset or classified information.*
- ◆ *It is recommended that supervisors ensure all personnel are aware of actions to take if hostile action or emergency situations occur which endangers classified/sensitive material or equipment.*
- ◆ *It is recommended that training be accomplished by conducting rehearsals of procedures and required actions to take in case of an emergency.*

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>PERSONNEL/INDUSTRIAL SECURITY</i></p>
<p><b><u>TOPIC:</u></b> <i>DOCUMENT CONTROL AND ACCOUNTABILITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>CLASSIFICATION AND MARKING</i></p>
<p><b><u>EXPLANATION:</u></b> Personnel/Industrial Security Classification and Marking refers to the security controls applied to documents containing sensitive information regarding critical assets through the classification of that information and the marking of documents.</p>
<p><b><u>INTENT:</u></b> To ensure that information associated with a critical asset that meets the criteria for classification is classified and protected to the appropriate level. Classification and Marking will also ensure that prescribed document classification and marking protocols are followed to alert document holders to the presence of sensitive or classified information and any special control or safeguarding requirements designed to help protect sensitive or classified information pertaining to critical assets against unauthorized dissemination.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Classification and Marking will review the use of prescribed document classification and marking protocols for documents containing sensitive or classified information associated with critical assets to include the use of document classification criteria, document marking requirements and the exercise of derivative classification responsibilities.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Personnel/Industrial Security Classification and Marking are based on guidelines contained in <i>DoD Critical Infrastructure Protection (CIP) Security Classification Guide (dated December 2003)</i>, <i>DoD 5220.22-M (NISPOM dated January 1995)</i>, <i>incorporating Change One (dated July 1997)</i> and <i>Change Two (dated February 2001)</i>, <i>DoDD 5220.22: DoD Industrial Security Program (dated December 1980)</i>, <i>DoD 5200.1PH: The DoD Guide to Marking Classified Documents (dated April 1997)</i> and <i>DoD Form 254: Contract Security Classification Specification (dated December 1999)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p>

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether the original classification of documents that pertain to a critical asset follow the criteria set forth in the *DoD CIP Security Classification Guide* as well as *NISPOM*. These documents contain specific criteria for determining whether information will be classified and a date or event for the duration of classification. Classification categories should follow guidelines set forth in *Executive Order (EO) 12958 as amended*.
  - ◆ *It is recommended that marking requirements for classified documents follow guidelines prescribed by the above references.*
  - ◆ *It is recommended that derivative classification responsibilities be authorized by the FSO and will follow guidance outlined in DoD 5200.1-PH.*

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

**AREA OF CONCERN:**

*PERSONNEL/INDUSTRIAL SECURITY*

**TOPIC:**

*DOCUMENT CONTROL AND ACCOUNTABILITY*

**SUBTOPIC:**

*SAFEGUARDING PROCEDURES*

**EXPLANATION:**

Document Control and Accountability Safeguarding Procedures refer to the information management system used by facilities to assure that the storage, access control, security checks, transmission, reproduction and destruction of classified documents forecloses the possibility of its loss or compromise.

**INTENT:**

To ensure that the information management system used for the protection and accountability of classified materials within a facility housing a critical asset will provide access controls to prevent non-authorized personnel from achieving access to classified information pertaining to the critical asset.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of Safeguarding Procedures will review a facility's information management system to determine the degree of effectiveness of access controls and other procedures to include physical/perimeter controls and security checks, emergency procedures, transmittal, transfer and dissemination procedures, process procedures, storage equipment requirements and the reproduction, retention and destruction of classified materials.

**CRITERIA:**

*The standards for the assessment of Safeguarding Procedures are based on the NISPOM (dated January 1995), Incorporating Change One (dated July 1997) and Change Two (dated February 2001). This reference addresses the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.*

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether end of the day security checks have been established to ensure that all critical asset classified materials (e.g., documents, diskettes, classified waste, etc.) have been returned to the originator, shredded or stored in a General Services Administration (GSA) approved security container (i.e., safe).

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

2. The assessor must verify whether perimeter controls have been established to deter and detect unauthorized introduction or removal of classified material from a facility housing a critical asset.
3. The assessor must verify whether a restricted area has been established to ensure controlled access to a critical asset's classified material in an open area during working hours, when it is impractical or impossible to protect classified material because of its size, quantity or other unusual characteristic.
  - ◆ *It is recommended that the restricted area have a clearly defined perimeter, but physical barriers are not required. Personnel within the area will be responsible for challenging all persons who may lack appropriate access authority.*
4. The assessor must verify whether intrusion detection systems (IDS) follow specified minimum standards set forth in the *NISPOM, Section 5-900*.
5. The assessor must verify whether automated access control systems or devices are capable of identifying the individual entering the area and authenticating that person's authority to enter the area.
  - ◆ *It is recommended that identification of individuals entering the area be obtained by an identification (ID) badge or card or by personal identification.*
6. The assessor must verify whether emergency procedures have been established that specify methods for emergency destruction, emergency evacuation and precautionary destruction of classified material and equipment that pertains to critical assets.
7. The assessor must verify whether external receipt and dispatch records are maintained.
8. The assessor must verify whether during the receipt of classified materials, all documentation is delivered directly to designate personnel.
  - ◆ *It is recommended, when U.S. Registered Mail, U.S. Express Mail, U.S. Certified Mail or classified material delivered by messenger is not received directly by designated personnel, procedures be established to ensure that the material is received by authorized persons for prompt delivery or notice to authorized personnel.*
9. The assessor must verify whether storage, transmission, reproduction and destruction processes and procedures have been established and are effectively executed to ensure the information management system will provide access controls to prevent non-authorized personnel from achieving access to classified information pertaining to the critical asset.
  - ◆ *It is recommended that storage procedures meet the established uniform requirements for the physical protection of CONFIDENTIAL, SECRET, and TOP SECRET materials as set forth in the NISPOM.*

**For Official Use Only**  
**Draft CIP FSVA Personnel/Industrial Security Standards**

- ◆ *It is recommended that construction of closed areas is necessary for storage when GSA-approved security containers or vaults are unsuitable or impractical. In such cases, construction requirements for closed areas and vaults should conform to the requirements of the NISPOM.*
- ◆ *It is recommended that transmission of classified materials pertaining to critical assets follows NISPOM guidelines that address preparation and receipting of classified materials, transmission of CONFIDENTIAL, SECRET and TOP SECRET materials within and outside of a critical asset facility, addressing classified materials and the use of couriers, hand carriers and escorts.*
- ◆ *It is recommended that a reproduction control system ensures that the reproduction of classified material associated with a critical asset is held to a minimum consistent with contractual and operational requirements.*
- ◆ *It is recommended that destruction and retention of classified material pertaining to a critical asset complies with established procedures for review of classified holdings on a recurring basis to reduce classified inventories to the minimum necessary for effective and efficient operations.*

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

**SAFETY STANDARDS**

**DESCRIPTION:**

Safety includes a consideration of the plans, policies, procedures, and training established to promote the safety of personnel assigned to critical assets.

<b><u>AREA OF CONCERN:</u></b> <i>SAFETY</i>
<b><u>TOPIC:</u></b> <i>SAFETY IN THE OPERATING ENVIRONMENT</i>
<b><u>SUBTOPIC:</u></b> <i>FACILITY LIFE SAFETY</i>
<b><u>EXPLANATION:</u></b> Facility Life Safety refers to the policies, plans, and procedures that are established to provide a safe operating environment for personnel working with or at a critical asset.
<b><u>INTENT:</u></b> To confirm that appropriate health and safety plans and procedures are in place to protect the personnel working with or at a critical asset, and to help preclude disruption of the critical asset.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Facility Life Safety will include a review of protective measures and devices used to ensure the safety of personnel working with or at a critical asset. Specifically, the review will cover walking and working surfaces, means of egress, occupational health and environmental control, hazardous materials, general environmental controls, fire protection, materials handling and storage, electrical systems, and toxic and hazardous substances.
<b><u>CRITERIA:</u></b> The standards for the assessment of Facility Life Safety are based on <i>29 CFR 1910: The Occupational Safety and Health Standards (OSHA)(undated)</i> . This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether Facility Life Safety plans and procedures are in place to protect the personnel working with or at a critical asset, and to help preclude disruption of the critical asset.
2. The assessor must verify the assessment of the following areas as appropriate, using *29 CFR 1910: OSHA Standards*:
  - a. Walking and Working Surfaces – Subpart D
  - b. Means of Egress – Subpart E
  - c. Occupational Health and Environmental Control – Subpart G
  - d. Hazardous Materials – Subpart H
  - e. General Environmental Controls – Subpart J
  - f. Fire Protection – Subpart L
  - g. Materials Handling and Storage – Subpart N
  - h. Electrical – Subpart S
  - i. Toxic and Hazardous Substances – Subpart Z
3. The assessor must verify whether Critical assets relating to construction, shipyards, marine terminals and longshoring use the following standards:
  - a. Construction – *29 CFR 1926: Safety and Health Standards for Construction*
  - b. Shipyards – *29 CFR 1915: Occupational Safety and Health Standards for Shipyard Employment*
  - c. Marine Terminals – *29 CFR 1917: Marine Terminals*
  - d. Longshoring – *29 CFR 1918: Safety and Health Standards for Longshoring*
4. Critical assets, especially in sensitive areas, will be protected by up-to-date fire detection and suppression systems.
5. The assessor must verify whether safety inspections of critical assets and their immediate environments are being conducted annually.

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

<p><b><u>AREA OF CONCERN:</u></b></p> <p>SAFETY</p>
<p><b><u>TOPIC:</u></b></p> <p>SAFETY IN THE OPERATING ENVIRONMENT</p>
<p><b><u>SUBTOPIC:</u></b></p> <p>EQUIPMENT/OPERATOR SAFETY</p>
<p><b><u>EXPLANATION:</u></b></p> <p>Equipment/Operator Safety refers to the safety standards that apply to specific critical asset equipment or personnel operating that equipment in or around a critical asset.</p>
<p><b><u>INTENT:</u></b></p> <p>To confirm that appropriate health and safety plans and procedures are in place to protect the personnel working with or at a critical asset, and to help preclude disruption of the critical asset.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of Equipment/Operator Safety will include a review of protective measures and devices used to ensure the safety of personnel working with or at a critical asset. Specifically, the review will cover personal protective equipment (PPE), machinery and machine guarding, handheld equipment, electrical systems, welding, cutting and brazing, and medical personnel and equipment.</p>
<p><b><u>CRITERIA:</u></b></p> <p>The standards for the assessment of Equipment/Operator Safety are based on the <i>Department of Defense Instruction (DoDI) 6055.1: DoD Safety and Occupational Health Program (dated 19 August 1998)</i> and <i>29 CFR 1910: The Occupational Safety and Health Standards (undated)</i>. These references address the required areas for assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify the following areas will be assessed at all critical assets, as appropriate for Equipment/Operator Safety, using <i>29 CFR 1910: OSHA Standards</i>:<ol style="list-style-type: none"><li>a. Personal Protective Equipment (PPE) – Subpart I<ol style="list-style-type: none"><li>(1) For critical assets, PPE should always include equipment for protection in the event of a chemical, biological or radiological incident, regardless of whether it is determined that these hazards are present or are likely to be introduced as a result of a deliberate attack or accidental release.</li></ol></li></ol></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

- (2) Assessment teams will review the type, quantity and condition of PPE maintained on site for use in the event of a chemical, biological or radiological incident.
  - b. Machinery and Machine Guarding – Subpart O
  - c. Hand and Portable Powered Tools and Other Handheld Equipment – Subpart P
  - d. Electrical – Safeguards for personnel protection – 29 CFR 1910.335
  - e. Welding, Cutting, Brazing – Subpart Q
2. The assessor must verify critical assets relating to construction, shipyards, marine terminals and longshoring use the following standards for Equipment/Operator Safety:
  - a. Construction – 29 CFR 1926: *Safety and Health Standards for Construction*
  - b. Shipyards – 29 CFR 1915: *Occupational Safety and Health Standards for Shipyard Employment*
  - c. Marine Terminals – 29 CFR 1917: *Marine Terminals*
  - d. Longshoring – 29 CFR 1918: *Safety and Health Standards for Longshoring*
3. The assessor must verify whether managers and supervisors ensure that personnel working with or at a critical asset follow safety standards and prevent and report accidents and workplace illness.
  - ◆ *It is recommended that evidence of this include documentation of any reports from workplace personnel or procedures for ensuring that personnel know when and to whom to report such incidents.*
4. The assessor must verify whether non-supervisory personnel ensure proper use of personal protective equipment and clothing and prompt reporting of unsafe conditions, hazardous exposure or occupational injury or illness that may impede the performance or capability of personnel operating or controlling critical assets.
  - ◆ *It is recommended that evidence of this include documentation of any unsafe condition or hazardous exposure reports from workplace personnel or procedures for ensuring that personnel know when and to whom to report such incidents.*
5. The assessor must verify whether Medical and First Aid personnel and equipment are in compliance with 29 CFR 1910, Subpart K.

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

<p><b><u>AREA OF CONCERN:</u></b></p> <p>SAFETY</p>
<p><b><u>TOPIC:</u></b></p> <p>SAFETY IN THE OPERATING ENVIRONMENT</p>
<p><b><u>SUBTOPIC:</u></b></p> <p>AMMUNITIONS AND EXPLOSIVES SAFETY</p>
<p><b><u>EXPLANATION:</u></b></p> <p>Ammunition and Explosives Safety for critical assets pertains to the establishment of uniform safety standards and preventative measures applicable to ammunition and explosives. In addition, it applies to associated personnel and property, as well as personnel and property exposed to the potential damaging effects of an accident involving ammunition and explosives during their development, manufacturing, testing, transportation, handling, storage, maintenance, demilitarization and disposal.</p>
<p><b><u>INTENT:</u></b></p> <p>To confirm that procedures and practices are in place to provide a critical asset the maximum possible protection from the damaging effects of potential accidents involving Ammunition and Explosives Safety.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of Ammunition and Explosives Safety will include a review of the preventative measures taken in the areas of storage facilities, electrical standards and fire prevention management.</p>
<p><b><u>CRITERIA:</u></b></p> <p>The standards for the assessment of Ammunition and Explosives Safety are based on guidelines contained in <i>Department of Defense Standard (DoD) 6055.9: Explosives Safety Standards and Department of Defense Standard (DoD-STD) (dated August 1997)</i> and <i>Department of the Army Pamphlet (DA Pam) 385-64: Ammunition (dated December 1999)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether construction of ammunition and explosives storage facilities, barricades and earth cover for magazines, policy on protective construction, facilities site criteria and general construction plans review for critical assets complies with <i>DoD-STD 6055.9, Chapter 5</i>.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

2. The assessor must verify whether critical assets that house ammunitions and explosives comply with the National Electrical Code and standards set for the in *DoD-STD 6055.9* for the design and installation of electrical equipment and wiring.
3. The assessor must verify whether all wiring and electrical equipment in underground storage facilities that are designated as critical assets are composed of moisture and corrosion resistant materials and construction.
  - ◆ *It is recommended that underground facilities have emergency lighting systems to provide minimum illumination in the event of a power failure.*
4. The assessor must verify whether personnel and equipment in hazardous locations and locations where static sensitive electro-explosive devices (EEDs) are exposed are grounded in a manner to discharge static electricity to prevent accumulations that are capable of igniting the dusts, gases and vapors that are exposed in or around a critical asset.
5. The assessor must verify whether electrical supply systems of critical assets housing ammunitions and explosives comply with guidelines set forth in *DoD STD 6055.9, Chapter 6*.
6. The assessor must verify whether Fire prevention management components include:
  - a. All operating personnel and firefighting forces involved with explosives are trained in the fire prevention precautions unique to fighting ammunition and explosive fires.
    - *It is recommended that this training will include the application and meaning of each type of fire hazard symbol, reporting fires, sounding alarms, area evacuations and type and use of appropriate firefighting equipment.*
  - b. Fire drills will be held within the explosives areas at acceptable intervals.
    - *It is recommended that fire drills will held at intervals of 6 months or less.*
    - *It is recommended that Frequent fire exit drills will be held and include the use of all emergency exits. All emergency exits will have exit signs that are clearly visible.*
    - *It is recommended that an audible, manually operated fire evacuation alarm system be installed in each building containing explosives. All alarm systems should be clearly labeled.*
7. The assessor must verify whether standards for maintenance and access to firefighting equipment follow standards set forth in *DA PAM 385-64, Section 3-9 through 3-12*.

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

- |   |
|---|
| <p>8. The assessor must verify whether inspection and maintenance of these systems conform to requirements of Technical Manual (TM) 5-695: <i>Maintenance of Fire Protection Systems</i>.</p> <p>9. The assessor must verify whether installations or activities responsible for critical assets that house ammunitions and explosives have developed Standard Operating Procedures (SOPs) or plans designed to provide safety, security and environmental protection.</p> <ul style="list-style-type: none"><li>◆ <i>It is recommended that plans be coordinated with the appropriate Federal, state and local emergency response authorities (e.g., law enforcement, fire departments hospitals, etc.) and any established Local Emergency Planning Committees (LEPCs). Minimum emergency standards are set forth in DA PAM 385-64, Section 3-24.</i></li></ul> |
|---|

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

<p><b><u>AREA OF CONCERN:</u></b> SAFETY</p>
<p><b><u>TOPIC:</u></b> SAFETY IN THE OPERATING ENVIRONMENT</p>
<p><b><u>SUBTOPIC:</u></b> FIRE PREVENTION</p>
<p><b><u>EXPLANATION:</u></b> Fire Prevention refers to the standards that apply to preventing fires at critical assets.</p>
<p><b><u>INTENT:</u></b> To confirm that appropriate fire prevention plans and procedures are in place to protect the health of the personnel working with or at a critical asset and to guard against critical asset equipment or materiel loss or damage.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Fire Prevention will include a review of a critical asset’s fire prevention plans and procedures.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Fire Prevention are based on <i>29 CFR 1910: OSHA Standards (undated)</i>. This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below. In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether Fire prevention plans have been established at critical assets and comply with standards set forth in <i>29 CFR 1910.39</i>.<ul style="list-style-type: none"><li>◆ <i>It is recommended that the fire prevention plan include the following elements:</i><ul style="list-style-type: none"><li>➤ <i>A list of all major fire hazards, proper handling and storage procedures for hazardous materials, potential ignition sources and their control and the type of fire protection equipment necessary to control each major hazard.</i></li><li>➤ <i>Procedures to control accumulations of flammable and combustible waste materials.</i></li><li>➤ <i>Procedures for regular maintenance of safeguards installed on heat-producing equipment to prevent the accidental ignition of combustible materials.</i></li><li>➤ <i>The name or job title of employees responsible for maintaining equipment to prevent or control sources of ignition or fires.</i></li></ul></li><li>◆ <i>It is recommended that the fire prevention plan is reviewed and updated annually.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Safety Standards**

<p><b><u>AREA OF CONCERN:</u></b></p> <p>SAFETY</p>
<p><b><u>TOPIC:</u></b></p> <p>TRAINING</p>
<p><b><u>SUBTOPIC:</u></b></p> <p>N/A</p>
<p><b><u>EXPLANATION:</u></b></p> <p>Safety Training refers to the training that personnel will receive with respect to the plans, policies and procedures established to promote the safety of personnel working with or at a critical asset.</p>
<p><b><u>INTENT:</u></b></p> <p>To ensure that the personnel working with or at a critical asset understand and have rehearsed the established safety procedures.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of Safety Training will include a review of training materials and records as well as spot checks of personnel to ensure that they have received the training.</p>
<p><b><u>CRITERIA:</u></b></p> <p>The standards for the assessment of Safety Training are based on <i>29 CFR 1910: OSHA Standards (undated)</i>. This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"> <li>1. The assessor must verify whether all employees receive safety training upon initial job assignment. <ul style="list-style-type: none"> <li>◆ <i>It is recommended that safety refresher training occur annually. It is recommended that evacuation rehearsals using both primary and alternate emergency exit routes will be conducted annually.</i></li> </ul> </li> </ol>

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

**PLANS STANDARDS**

**DESCRIPTION:**

Plans involve a consideration of written policies and procedures and the coordination necessary to help protect a critical asset through pre-incident emergency response planning, continuity of operations (COOP) planning and threat awareness. Plans cover emergency response actions to be taken by personnel assigned to work with or at a critical asset, actions to be taken by emergency first responders and those to be taken by supporting local, State and, if required, Federal response agencies and organizations. Plans also include intelligence sharing and liaison programs with supporting or neighboring agencies and organizations that ensure the organizations owning and maintaining critical assets are informed of current and emerging threat conditions. Plans also provide for the dissemination of security intelligence information regarding potential threats to the personnel assigned to operate or work with the critical asset.

<b><u>AREA OF CONCERN:</u></b> <i>PLANS</i>
<b><u>TOPIC:</u></b> <i>TRAINING</i>
<b><u>SUBTOPIC:</u></b> <i>EMERGENCY RESPONSE PLANNING - CRITICAL ASSET PERSONNEL</i>
<b><u>EXPLANATION:</u></b> Emergency Response Planning for Critical Asset Personnel refers to the planned actions to be taken by personnel assigned to work with or at a critical asset in the event of an emergency.
<b><u>INTENT:</u></b> To ensure that personnel assigned to work with or at critical assets are prepared to respond appropriately in the event of an emergency.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Emergency Response Planning area will include a review of the emergency response plans covering the critical asset that address actions to be taken by personnel working with or at a critical asset in the event of an emergency.

## For Official Use Only

### Draft CIP FSVA Plans Standards

#### **CRITERIA:**

The standards for the assessment of Emergency Response Planning for personnel assigned to work with or at a critical asset are based on 29 CFR 1910: *Occupational Safety and Health Standards (undated)*, *Federal Response Plan (FRP) 9230-1-PL (dated April 2003)*, and the *FEMA Disaster Mitigation Act of 2000*. These references collectively address the required areas for assessment of this subtopic.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether there is an established emergency response plan that covers the critical asset will address emergencies that the employer may reasonably expect at the critical asset (e.g., fire, toxic chemical releases, hurricanes, tornadoes, etc.).
  - ◆ *It is recommended that the emergency response plan that covers the critical asset includes the following procedures:*
    - *How to report a fire or other emergency.*
    - *Initiating distinctive alarms for different categories of emergency conditions in compliance with the requirements in 29 CFR 1910.165.*
    - *Emergency evacuation, including type of evacuation, exit route assignments and evacuation assembly areas.*
    - *Employees who remain to operate or shut down critical systems.*
    - *Employees performing rescue or medical duties.*
    - *Respond to Chemical, Biological Radiological Nuclear Explosive (CBRNE) incidents including procedures to communicate instructions to critical asset personnel, identifying shelter-in-place areas (if they exist) and identifying the selection and use of appropriate personal protective equipment.*
    - *Accounting for all employees after evacuation.*
2. The assessor must verify whether a responsible training official ensures that regularly prescribed and documented training in emergency response actions is conducted for all personnel working with or at the critical asset.
3. The assessor must verify whether a responsible training official ensures that the emergency response plan covering employee actions is reviewed and updated annually or when changing conditions require changes to the plan.

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

<p><b><u>AREA OF CONCERN:</u></b></p> <p><i>PLANS</i></p>
<p><b><u>TOPIC:</u></b></p> <p><i>EMERGENCY PREPAREDNESS</i></p>
<p><b><u>SUBTOPIC:</u></b></p> <p><i>EMERGENCY RESPONSE PLANNING – FIRST RESPONDERS</i></p>
<p><b><u>EXPLANATION:</u></b></p> <p>Emergency Response Planning for First Responders refers to the planning and coordination that the critical asset owners conduct in conjunction with fire and rescue, medical and law enforcement agencies.</p>
<p><b><u>INTENT:</u></b></p> <p>To confirm that sufficient coordination has been conducted between the critical asset owners and first responders (i.e., fire and rescue, medical, and law enforcement) to ensure that all parties are prepared to respond rapidly to emergencies affecting the critical asset.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of the Emergency Response Planning for First Responders will include a review of all plans, MOU/MOA, and coordination measures in place between the critical asset owners and first responders to ensure continuous support and prompt response.</p>
<p><b><u>CRITERIA:</u></b></p> <p>The standards for the assessment of Emergency Response Planning for First Responders are based on guidelines contained in the <i>FRP 9230-1-PL (dated April 2003)</i> and the <i>FEMA Disaster Mitigation Act of 2000</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify if planning has been completed between critical asset owners and first responder authorities to ensure that critical asset(s) are supported in the event of an emergency.</li><li>2. The assessor must verify whether pre-event emergency planning for first responders includes:<ol style="list-style-type: none"><li>a. Verifying the capabilities of first responders supporting the designated critical asset.</li></ol></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

- b. Identifying potential emergency conditions that may require first responder support.
  - c. Verifying procedures for initiating first responder action in the event of an emergency.
  - d. Designating individuals within the personnel assigned to work with or at the critical asset who will assist and guide first responders upon arrival of first responder units on-site.
  - e. Verifying locations of key utilities (e.g., water mains, fire hydrants, HVAC shut-down systems, etc.) to which first responders may require access.
  - f. Procedures to be followed by critical asset personnel and first responders if the emergency requires responder access to classified or sensitive areas.
  - g. Verifying that redundant first responder capabilities are identified and coordinated to ensure support will be available if “first line” responders are committed to another emergency.
3. The assessor must verify whether critical asset facility and security managers conduct continuous coordination with supporting first responder agencies.
  4. The assessor must verify whether supporting first responder organizations are included in any exercise of the critical asset’s emergency response plans.
  5. The assessor must verify whether emergency response plans that involve first responders are reviewed and updated annually or as exercise lessons learned or changes to conditions or first responder supporting relationships occur.

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

<p><b><u>AREA OF CONCERN:</u></b></p> <p><i>PLANS</i></p>
<p><b><u>TOPIC:</u></b></p> <p><i>EMERGENCY PREPAREDNESS</i></p>
<p><b><u>SUBTOPIC:</u></b></p> <p><i>EMERGENCY RESPONSE PLANNING - SUPPORTING LOCAL, STATE, AND FEDERAL RESPONSE AGENCIES</i></p>
<p><b><u>EXPLANATION:</u></b></p> <p>Emergency Response Planning for Supporting Local, State, and Federal Response Agencies refers to planning and coordination conducted to ensure support from those organizations that may respond to an event at a critical asset in lieu of or in support of the first responders.</p>
<p><b><u>INTENT:</u></b></p> <p>To confirm that sufficient coordination has been conducted between the critical asset owners and supporting Local, State, and Federal response agencies and organizations to ensure that all parties are prepared to respond rapidly to emergencies affecting the critical asset.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of the Emergency Response Planning for Supporting Local, State, and Federal Response Agencies will include a review of all plans, MOU/MOA and coordination measures in place between the critical asset owners and supporting local, State and Federal response agencies and organizations to ensure continuous support and prompt response.</p>
<p><b><u>CRITERIA:</u></b></p> <p>The standards for assessment of supporting Local, State, and Federal response agencies are based on guidelines contained in the <i>FRP 9230-1-PL (dated April 2003)</i> and the <i>FEMA Disaster Mitigation Act of 2000</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must determine if planning has been completed with local, State or Federal agencies and organizations that support first responders to ensure that critical assets will be supported in the event that an incident response requirement exceeds the capability of the designated first responders.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

2. The assessor must verify that pre-emergency planning includes:
  - a. Verifying the limits of first responder capabilities as defined in emergency response support.
  - b. Identifying potential emergency conditions that may require emergency response support beyond that available through first responders.
  - c. Determining the capabilities that may be required of agencies that may support or augment first responders.
  - d. Determining support relationships between first responders and supporting Local, State, and Federal emergency response agencies, organizations (including the Federal Emergency Response Team [ERT]) and setting priorities to ensure redundant and continuous support to critical assets.
3. The assessor must verify whether critical asset facility and security managers conduct continuous coordination with supporting local, State and Federal response agencies and organizations.
4. The assessor must verify whether support to critical assets is integrated into larger State and Federal emergency response exercises.
5. The assessor must verify whether emergency response plans for supporting Local, State, and Federal agencies are updated from exercise lessons learned or, as changing conditions and supporting relationships occur.

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

<p><b><u>AREA OF CONCERN:</u></b></p> <p><i>PLANS</i></p>
<p><b><u>TOPIC:</u></b></p> <p><i>EMERGENCY RESPONSE PLANNING</i></p>
<p><b><u>SUBTOPIC:</u></b></p> <p><i>CONTINUITY OF OPERATIONS (COOP)</i></p>
<p><b><u>EXPLANATION:</u></b></p> <p>Continuity of Operations (COOP) refers to the planning and coordination conducted to ensure the continued operation of critical assets in the event of an emergency incident that occurs with or without warning. The nature of the possible emergencies include man-made and naturally occurring events and may run from catastrophic events that cause long-term interruption of operations to less significant events that cause short-term interruptions.</p>
<p><b><u>INTENT:</u></b></p> <p>To ensure that critical asset owners are prepared to sustain critical asset functions and operations in an all-hazards environment.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of the COOP area will include a review of COOP plans and the level of coordination completed by critical asset owners to ensure the plan(s) can be successfully executed if required. An assessment will also ensure that critical asset COOP planning considers the full range of categories of potential threats to the critical asset, including both man-made and naturally occurring events.</p>
<p><b><u>CRITERIA:</u></b></p> <p>The standards for the assessment of COOP are based on guidance contained in <i>FEMA Federal Preparedness Circular (FPC) 65: Federal Executive Branch Continuity of Operations (dated 26 July 1999)</i>, <i>FRP 9230.1 PL (dated April 2003)</i>, the <i>FEMA Disaster Mitigation Act of 2000</i>, and Federal agency COOP and disaster response plans and programs. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must assess a critical asset's COOP capability to include a review of the critical asset's COOP Plan.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

2. The assessor must verify whether the critical asset's COOP Plan ensures redundancy of critical systems to ensure that essential operations can be sustained in the event of a sudden disruption.
- ◆ *It is recommended that the COOP Plan include the following:*
    - *A COOP program manager or equivalent should be identified and be responsible for the maintenance of the COOP Plan.*
    - *COOP planning should include all necessary actions required to ensue the continuous operation of the critical asset, whether operations can be maintained at the normal critical asset site or if relocation to an alternate site is required.*
    - *COOP planning should ensure that alternate site operation, if required, will be established within 12 hours after an emergency event occurs. If an alternate facility is required, that site will be identified in the plan and sufficiently resourced to support sustained operations.*
    - *The COOP alternate site should have security countermeasures and personnel safety measures in place that permit the alternate site to meet or exceed the level of security of the primary critical asset site.*
    - *The COOP Plan should outline procedures for implementation with or without warning and during normal work hours or during non-work hours.*
    - *Critical asset owners should establish a multi-year strategic and program management plan to ensure sufficient resources are maintained to support the COOP Plan.*
    - *Personnel assigned to work with or at a critical asset should receive periodic training in the COOP Plan and all associated plans and procedures should be rehearsed.*

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

<p><b><u>AREA OF CONCERN:</u></b></p> <p><i>PLANS</i></p>
<p><b><u>TOPIC:</u></b></p> <p><i>INTELLIGENCE SHARING</i></p>
<p><b><u>SUBTOPIC:</u></b></p> <p><i>COORDINATION WITH EXTERNAL AGENCIES</i></p>
<p><b><u>EXPLANATION:</u></b></p> <p>Intelligence Coordination with External Agencies refers to the planning and coordination with law enforcement agencies, including Local, State, Federal, or host nation law enforcement services, to ensure that critical asset security managers and responsible authorities are informed of the current or emerging threat environment. Intelligence coordination with external agencies also refers to evaluating impediments or disincentives to security-related information sharing and developing and facilitating reliable and secure communications to support information sharing pertaining to security measures for critical assets among law enforcement agencies and Local, State, Federal, and host nation governments.</p>
<p><b><u>INTENT:</u></b></p> <p>To ensure that critical asset security managers and responsible authorities coordinate with local, State and Federal law enforcement agencies to be informed of relevant potential threats and prepared to direct appropriate actions to protect critical assets from potential or imminent threats.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of Intelligence Coordination with External Agencies that pertains to critical assets will include a review of ongoing planning and coordination that is conducted with local, State, Federal or host nation law enforcement or security agencies.</p>
<p><b><u>CRITERIA:</u></b></p> <p>Where specific documentary sources of assessment guidelines are not identified, as in the case of Intelligence Coordination with External Agencies, standards for assessment are based on an analysis of findings and lessons learned from vulnerability assessments of a variety of government department and agency facilities and assets.</p>

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether critical asset security managers conduct continuous coordination with local law enforcement agencies to receive information regarding current and projected threat activities that may affect critical assets.
  - ◆ *It is recommended that security managers also request threat information pertaining to potential damage or compromise of critical assets from State or national level law enforcement agencies. Critical asset security managers should query external sources of supply and services including the supporting infrastructures (e.g.*
2. The assessor must verify whether critical asset security managers have developed a network of relationships with security managers of other critical assets, organizations or facilities within the local area of interest and share intelligence information on a recurring basis.
  - ◆ *It is recommended that critical asset security managers participate, as appropriate, in area management councils that promote the sharing of local or regional threat intelligence information pertaining to the protection of critical assets.*

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

<p><b><u>AREA OF CONCERN:</u></b></p> <p>PLANS</p>
<p><b><u>TOPIC:</u></b></p> <p>INTELLIGENCE SHARING</p>
<p><b><u>SUBTOPIC:</u></b></p> <p>INTERNAL DISSEMINATION OF SECURITY INTELLIGENCE</p>
<p><b><u>EXPLANATION:</u></b></p> <p>Internal Dissemination of Security Intelligence refers to the planning and coordination conducted to enable the dissemination of the appropriate level of threat and security countermeasure information to personnel assigned to work with or at critical assets. Plans also include provisions for informing personnel working with or at a critical asset of actions they are expected to take to guard against emerging threats.</p>
<p><b><u>INTENT:</u></b></p> <p>To ensure that an appropriate level of threat information is provided to personnel working with or at a critical asset as a means to enlist their assistance and support of critical asset protection countermeasures.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of plans for the Internal Dissemination of Security Intelligence will include a review of ongoing planning and coordination for providing appropriate information to personnel working with or at a critical asset regarding the threat level and security measures taken to protect critical assets.</p>
<p><b><u>CRITERIA:</u></b></p> <p>Where specific documentary sources of assessment guidelines are not identified, as in the case of Internal Dissemination of Security Intelligence, standards for assessment are based on an analysis of findings and lessons learned from vulnerability assessments of a variety of government department and agency facilities and assets.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether an appropriate level of threat information is provided to personnel working with or at a critical asset as a means to enlist their assistance and support of critical asset protection countermeasures.<ul style="list-style-type: none"><li>◆ <i>It is recommended that critical asset security managers brief their senior management on the existing threat situation on an as needed basis and provide recommendations regarding actions to be taken to minimize threats.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Plans Standards**

- ◆ *It is recommended that critical asset owners have a mechanism or process in place to identify changes to the local threat condition, assess the potential impact on the organization's critical assets, approve the use of additional countermeasures and approve the internal media message to be provided to the personnel working with or at the critical asset.*
- ◆ *It is recommended that mechanisms exist to transmit threat information pertaining to critical assets to all personnel and to indicate:*
  - *Changes to the announced threat level.*
  - *Additional countermeasures that will be activated that may impact on "normal" operations.*
  - *Additional behavioral requirements expected of personnel assigned to work with or at a critical asset to address the new threat condition.*

**For Official Use Only**  
**Draft CIP FSVA Operations Security Standards**

**OPERATIONS SECURITY**

**DESCRIPTION:**

Operations Security (OPSEC) includes a consideration of the processes and procedures by which critical information is identified and protected against exploitation by an adversary.

<b><u>AREA OF CONCERN:</u></b> <i>OPERATIONS SECURITY (OPSEC)</i>
<b><u>TOPIC:</u></b> <i>INFORMATION MANAGEMENT</i>
<b><u>SUBTOPIC:</u></b> <i>N/A</i>
<b><u>EXPLANATION:</u></b> Operations Security (OPSEC) is an analytic process used to deny an adversary, information concerning intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations. OPSEC does not replace other security disciplines – OPSEC supplements them.
<b><u>INTENT:</u></b> To ensure that access to critical infrastructure asset information is protected from our adversaries, and to restrict access to those individuals that have a need to know.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of OPSEC will include reviews of the OPSEC Program, OPSEC Planning and Website OPSEC.
<b><u>CRITERIA:</u></b> The standards for the assessment of OPSEC Information Management are based on <i>DOD OPSEC Directive 5205.2 (dated 29 November, 1999), Army Operations Security: AR 530-1 3 (dated 3 March, 1995), Air Force Program AFI 10-1011: Operations Security (dated 31 May 2001), Identification of Critical Information AFI 10-1101: Operations Security (dated 31 May 2001), General Web Site OPSEC, DOE OPSEC and NSA IOSS.</i>  In support of a given mission and where applicable, the FSIVA assessor must verify the following:

**For Official Use Only**  
**Draft CIP FSVA Operations Security Standards**

1. The assessor must verify whether there is an OPSEC Program established to ensure that access to critical infrastructure asset information is protected from our adversaries, and to restrict access to those individuals that have a need to know.
  - ◆ *It is recommended that the OPSEC program:*
    - *Assignment of responsibility for OPSEC direction and implementation.*
    - *Issuance of procedures and planning guidance for the use of OPSEC techniques to identify vulnerabilities and apply applicable countermeasures.*
    - *Establishment of OPSEC education and awareness training. Training programs should ensure that all personnel, commensurate with their positions and security clearance, are aware of adversary intelligence threats and understand the OPSEC process.*
    - *Annual review and validation of OPSEC plans and programs.*
    - *Special requirements to plan for and implement OPSEC before, during and after operations and other activities.*
2. The assessor must verify whether OPSEC Planning is included as part of the overall planning cycle associated with critical assets and will include a formalized process.
  - ◆ *It is recommended that the OPSEC process consist of five distinct actions: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk and application of appropriate OPSEC measures.*
3. The assessor must determine the degree to which procedures have been implemented to identify critical information associated with the asset.
  - ◆ *It is recommended that organizations and activities associated with the critical asset be apprised of operational information determined to be critical so that they too can protect this information as well as any associated indicators.*
  - ◆ *It is recommended that requirements to control and protect critical information will be identified to contractors.*
  - ◆ *It is recommended that contractors continue to control and protect critical information until the need for OPSEC measures no longer exist.*
4. The assessor must identify the procedures in place at the critical asset to ensure the analysis of threats to the critical asset.
5. The assessor must determine the degree to which procedures have been implemented at the critical asset to ensure that vulnerabilities are analyzed to determine which OPSEC measure provide the needed protection at the least cost to operational efficiency.

**For Official Use Only**  
**Draft CIP FSVA Operations Security Standards**

6. The assessor must determine if the critical asset has procedures in place to assess risks. Based on the risk assessment, a decision will be made as to which OPSEC measures to implement and when to do so. An analysis will be done to determine the interaction of OPSEC measures will be to ensure that a measure to protect a specific piece of critical information does not unwittingly provide and indicator of another.
7. The assessor must identify the degree to which those OPSEC measures that have been identified have been implemented at the critical asset.
8. The assessor must verify whether critical Assets have an OPSEC annex or plan.
  - ◆ *It is recommended that because there is no set format for an OPSEC Plan, the format and content of the OPSEC plan will be tailored to meet the specific need. The OPSEC plan will address the following points:*
    - *Requirements for essential secrecy about friendly intentions and capabilities from initial planning through post-execution phases.*
    - *Tasks to associated activities to plan and implement OPSEC measures.*
    - *An OPSEC estimate that includes identified or assumed adversary knowledge, Essential Elements of Friendly Information (EEFI) and an evaluation of OPSEC effectiveness.*
    - *The OPSEC threat, consisting of and adversary's intent and capability to obtain information.*
    - *OPSEC measures to be implemented.*
9. The assessor must verify whether periodic OPSEC program reviews are conducted to thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists.
  - ◆ *It is recommended that when applying the OPSEC process to information posted to Web sites, the activity will evaluate subject data as it relates to critical assets. This includes information concerning the asset, equipment, personnel or any information that when taken as a whole, may provide sensitive information about the critical asset. Evaluations of activity information provided on publicly accessible Web sites should follow current OPSEC methodology:*
    - *Identify information access points and evaluate their importance to activity operations.*
    - *Determine the critical information for the activity's operations and plans. Information that would not be of interest/use to the general public will not be on a public access page.*
    - *Determine the threat to the operation of the critical asset from the release of the information.*

**For Official Use Only**  
**Draft CIP FSVA Operations Security Standards**

- *Determine the vulnerabilities associated with the release of this information.*
  - *Assess the risk posed to the critical asset and determine what protection should be applied to minimize potential loss of critical information and what is the impact on operations and operations support.*
  - *Apply OPSEC measures to minimize information loss and vulnerability.*
10. The assessor must review the policies in place at the critical asset to ensure that responsibility for management of information placed on component websites has been assigned.
- ◆ *It is recommended that the designated individual will ensure that website owners take responsibility for all content posted to their websites. Website owners will:*
    - *Verify that there is a valid mission needed to disseminate the information to be posted.*
    - *Apply the OPSEC review process.*
    - *Limit details.*
    - *Use the required process for clearing information for public dissemination.*
    - *Protect information according to its sensitivity.*
    - *Ensure reviewing officials and webmasters are selected and have received appropriate training in security and release requirements.*
11. The assessor must verify whether the facility has established and follows sufficient website OPSEC to restrict access.
- ◆ *It is recommended that websites prominently display privacy and security notices on the main web page of all major sections of each website information service.*
  - ◆ *It is recommended that websites will not contain any personal identification information (e.g., Social Security Numbers, dates of birth, home addresses, etc.).*
  - ◆ *It is recommended that websites will not contain any technological data that may provide information about the critical asset that could be used alone, or in combination with other data, to determine sensitive information about the critical asset.*

**For Official Use Only**  
**Draft CIP FSVA Operations Security Standards**

<b><u>AREA OF CONCERN:</u></b> <i>OPERATIONS SECURITY (OPSEC)</i>
<b><u>TOPIC:</u></b> <i>TRAINING</i>
<b><u>SUBTOPIC:</u></b> <i>N/A</i>
<b><u>EXPLANATION:</u></b> OPSEC training refers to the training that employees and contractors supporting critical assets will receive regarding the concept of OPSEC and how to apply that knowledge and awareness in the performance of their day-to day tasks.
<b><u>INTENT:</u></b> To ensure that employees and contractors understand and acknowledge the operations security policies and procedures.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment will include a review of training schedules and training records to determine whether or not cleared personnel requiring access to critical assets and associated classified information have received, or are scheduled to receive, initial operations security briefs and refresher training.
<b><u>CRITERIA:</u></b> The standards for the assessment of Operations Security Training are based on guidelines contained in <i>OPSEC Practitioner's Toolbox (undated)</i> and <i>AR 530-1: Operations Security (3 March 1995)</i> . The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this topic.  In support of a given mission and where applicable, the FSIVA assessor must verify the following:  1. The assessor must verify whether proper procedures are followed to ensure employees and contractors understand and acknowledge the operations security policies and procedures. <ul style="list-style-type: none"><li>◆ <i>It is recommended that prior to being granted access to the critical asset(s) or associated sensitive information, an employee will receive an initial OPSEC briefing that includes the following:</i><ul style="list-style-type: none"><li>➤ <i>Information Assurance (IA) threat awareness briefing</i></li><li>➤ <i>An overview of the security classification system</i></li></ul></li></ul>

**For Official Use Only**  
**Draft CIP FSVA Operations Security Standards**

- *Employee reporting obligations and requirements*
- *Security procedures and duties applicable to the employee's job*
- *Initial OPSEC awareness orientation will cover all important OPSEC issues, as determined by the OPSEC manager*
- ◆ *It is recommended that personnel granted access to critical assets and classified information related to the asset will receive refresher security training annually.*
- ◆ *It is recommended that refresher training include the importance of sound OPSEC practices needed to deny or control information about critical assets and intentions from hostile intelligence activities. It is recommended that OPSEC Managers employ all means to ensure continuous OPSEC awareness is provided to personnel assigned to the critical asset(s).*
- ◆ *It is recommended that the OPSEC Manager ensure that all personnel, commensurate with their positions and security clearance, are aware of the adversary intelligence threats and understand the OPSEC process.*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

**SECURITY OF NUCLEAR CRITICAL ASSETS**

**DESCRIPTION:**

Nuclear Security Standards include the components of security that maximizes the safeguarding of nuclear weapons or their components and other nuclear materials by impeding or denying a potential intruder or adversary access to the weapon, components or material. The safety, security, control and effectiveness of nuclear weapons that are designated as critical assets are of paramount importance to the security of the United States.

<b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF NUCLEAR CRITICAL ASSETS</i>
<b><u>TOPIC:</u></b> <i>PERSONNEL RELIABILITY</i>
<b><u>SUBTOPIC:</u></b> <i>PERSONNEL RELIABILITY PROGRAM (PRP)</i>
<b><u>EXPLANATION:</u></b> Personnel Reliability Program (PRP) refers to the process of granting or denying individual access to sensitive information, equipment or materials that are associated with a critical asset based on investigations and verification of individual trustworthiness and loyalty.
<b><u>INTENT:</u></b> To ensure that access to restricted information, equipment or materials associated with a designated nuclear critical asset is limited to those personnel who require access and for whom investigations verifying their trustworthiness and loyalty have been completed.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the PRP for designated nuclear critical assets will include assessing the policies, responsibilities, procedures for management and standards of individual reliability in personnel performing duties associated with nuclear weapons and their components. Additionally, an assessment will be performed on the processes for the selection and retention of personnel. An assessment will also be made of the administration of the day-to-day functions of the PRP to include monitoring of the program, the dissemination of PRP information, the reviewing and certifying officials, commanders, supporting staff, indoctrination and training administrators on program objectives and procedures.

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

**CRITERIA:**

The standards for the assessment of the PRP are based on guidelines contained in *Department of Defense (DoD) 5210.42-R: Nuclear Weapons Personnel Reliability Program (dated 8 January 2001)*. This reference addresses all the required areas for the assessment of this subtopic. The baseline reference is supplemented as required and as indicated below.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether procedures exist for formally designating the reviewing officials and certifying officials.
  - ◆ *It is recommended that certifying officials be designated as "critical" or "controlled" PRP positions commensurate with the highest category of any critical asset duty position in the organization or activity.*
2. The assessor must verify whether procedures exist to appoint an agency or site Competent Medical Authority (CMA) to act as a PRP medical consultant to determine an individual's suitability to perform PRP duties that are directly related to critical assets.
3. The assessor must verify whether Subordinate organizations with large PRP populations appoint a PRP monitor(s) to administer the day-to-day functions of the PRP that are directly related to critical assets.
4. The assessor must verify whether reviewing officials, certifying officials, PRP monitors, CMAs and other medical personnel with responsibilities relating to critical assets receive initial and refresher PRP training and will be briefed on their PRP management and oversight responsibilities.
5. The assessor must verify whether organizations ensure that the PRP is reviewed and evaluated during assessments and staff visits at all levels of authority for personnel with duties and responsibilities related to critical assets.
  - ◆ *It is recommended that the results of those assessments be reviewed at the highest level of authority.*
6. The assessor must verify whether the certifying official is familiar with and applies the Reliability Standards as they direct PRP qualifying standards, disqualifying or decertifying standards.
7. The assessor must verify whether PRP screening procedures exist and will rest with the certifying official for initial acceptability for assignments of PRP positions.

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- ◆ *It is recommended that individuals responsible for or who have duties related to designated critical assets that fail to meet the specified reliability standards not be assigned to or continued in duties of a PRP position. A certification of PRP acceptability should be revoked immediately on a certifying official's determination that an individual no longer meets the standards.*
8. The assessor must verify whether certifying officials for contractors who are responsible for or have duties relating to designated nuclear critical assets and whose duties are subject to the PRP ensure that contracts require that contractor employees performing duties in PRP positions meet the reliability standards of the PRP.
9. The assessor must verify whether medical personnel providing PRP support are given an initial and periodic orientation in nuclear weapon operations that relate to designated critical assets, emphasizing safety and security aspects and the responsibility for advising designated authorities of medical conditions that adversely affect the certification of unit security force personnel.
- ◆ *It is recommended that there be close cooperation and coordination between the organization and designated support medical activity to assure continuing application of the PRP.*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF NUCLEAR CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>NUCLEAR FACILITY SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Nuclear Facility Security refers to the system and procedures established to prevent the loss, threat, unauthorized access and use, sabotage or destruction of a particular space, structure or facility containing nuclear weapons or nuclear material that are designated as critical assets.</p>
<p><b><u>INTENT:</u></b> Nuclear security measures for facilities will ensure that the nuclear weapons, components or other nuclear material that are designated as critical assets will not be subject to loss, theft, sabotage, unauthorized use, unauthorized destruction, unauthorized disablement or accidental damage. The safety, security, control and effectiveness of nuclear weapons designated as critical assets are of paramount importance to the security of the United States.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Nuclear Facility Security measures will include assessing the measures designed to safeguard and protect the critical asset from access by unauthorized individuals or potential adversaries. This will include examining the overall security posture of the critical asset by reviewing the security plans and procedures that are in place, assessing the effectiveness of the security force protecting the facility, the use of physical features outside and within the perimeter of the facility and the technical devices or other security measures that impede or hinder potential intruders or adversaries from gaining access to the critical asset.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Nuclear Facility Security are based on guidelines contained in <i>DoD C-5210.41-M/Air Force Supplement: Nuclear Weapons Security Manual (dated 1 September 1999)</i>. This reference addresses all the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.  In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p>

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

1. The assessor must verify whether security patrols inspect all areas of possible concealment in and around the critical asset for indications that unauthorized personnel use these areas for observation and surveillance of facility operations.
  - ◆ *It is recommended that checks be made at random routes at least once daily. This check will include the facility perimeter that will be randomly checked for integrity (e.g., no breaks in the fence, no evidence of attempted penetrations, etc.).*
2. The assessor must verify whether exterior inspections of all structures containing designated critical assets conducted for signs of tampering and covert entry.
  - ◆ *It is recommended that the result of the inspections be annotated in the guard force blotter or other suitable form.*
3. The assessor must verify whether inspections are conducted in permanent restricted areas containing nuclear resources that are designated as critical assets.
  - ◆ *It is recommended that this inspection ensures that the underbrush in no higher than eight inches within the restricted area, clear zones and between fences.*
4. The assessor must verify whether inspections are performed to ensure that nuclear resources and facilities containing nuclear resources that are designated as critical assets are located an acceptable distance inside the restricted area boundary.
  - ◆ *It is recommended that where the critical asset or facility that houses a critical asset restricted area boundary is 250 feet or more from the base perimeter or property line, inspections will be performed and action will be taken to ensure that nuclear resources and facilities containing nuclear resources that are designated as critical assets are located a minimum of 50 feet inside the restricted area boundary and for double fences, 50 feet inside the inner fence.*
  - ◆ *It is recommended that action be taken to ensure that there are two boundary fences around the designated nuclear critical asset separated not less than 30 feet and not more than 150 feet. For Continental United States (CONUS) facilities, single boundary fences should be permitted.*
5. The assessor must verify whether openings that pass through or under the critical asset boundary barriers are secured.
6. The assessor must verify whether measures have been taken to prevent unauthorized landing of aircraft or other airborne assault techniques into the limited/restricted areas around the critical asset for the purpose of gaining access to or effecting removal of a nuclear weapon/material.

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

7. The assessor must verify whether security plans provide for continuous intrusion detection and surveillance at the boundary of the critical asset or for the use of posted sentries when the intrusion detection system (IDS) is not installed or operational.
8. The assessor must verify whether sensors on the nuclear designated critical asset area perimeter, fence line, clear zones(s) or around exposed critical assets are emplaced so that they will detect walking, running, rolling, crawling across or jumping through the line of detection, cutting, climbing on or lifting the fence fabric.
9. The assessor must verify whether sensors located at designated nuclear critical assets (e.g., structures, shelters, etc.) are emplaced so that they detect intrusion attempts through the doors, walls, roofs or vents before an intruder reaches the critical asset.
  - ◆ *It is recommended that structures without substantially constructed walls will have IDS coverage of the walls and roof.*
10. The assessor must verify whether sufficient response procedures are in place if a single line of interior IDS exceeds false or nuisance alarm rates, to dispatch an internal Security Response Team (SRT) to conduct an exterior sweep of the affected critical asset to ensure there are no signs of forced entry.
11. The assessor must verify whether sufficient data transmission line supervision features and security force surveillance are in place to protect data transmission equipment against tampering.
12. The assessor must verify whether IDS cables supporting an intrusion detection system for a designated nuclear critical asset that are not directly protected by sensors are sufficiently protected.
  - ◆ *It is recommended that IDS cables supporting an intrusion detection system for a designated nuclear critical asset that are not directly protected by sensors, be routed through metal conduit either buried to the normal depth of cables or suspended at least ten feet above the surface.*
13. The assessor must verify whether all equipment that terminates, splices, or groups interior or exterior IDS inputs for a nuclear critical asset is sufficiently protected against tampering.
  - ◆ *It is recommended that all equipment that terminates, splices, or groups interior or exterior IDS inputs for a nuclear critical asset be with installed locks and tamper switches that provide a tamper indication at the annunciator. Tamper switches are not required if the equipment is located within the protection zone of the sensors but they will be locked or sealed.*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- |  |
|--|
| 14. The assessor must verify whether adequate compensatory measures are applied when any portion of the IDS for a nuclear critical asset fails or has been accessed. |
|--|

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF NUCLEAR CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>NUCLEAR WEAPON SYSTEM SAFETY</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Nuclear Weapon System Safety refers to the special safety considerations involving material, personnel and procedures associated with critical assets that contribute to the security and safety of nuclear weapon systems and to the assurance that there will be no nuclear weapon accidents, incidents or unauthorized weapon detonations.</p>
<p><b><u>INTENT:</u></b> To ensure that the rules governing safety of nuclear weapon systems that are designated as critical assets provide the maximum protection possible against the risks and threats inherent in today's environment to personnel, the general environment and surrounding communities.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of a designated nuclear critical asset's safety will include an assessment of the existing measures that are in place designed to prevent an unexpected event involving nuclear or radiological weapon components designated as critical assets that may result in radioactive contamination or the seizure, theft, loss or destruction of a nuclear or radiological weapon component that would create a public hazard, actual or implied.</p>
<p><b><u>CRITERIA:</u></b> The standard for the assessment of nuclear weapon system safety is based on <i>DoD Directive 3150.2-M: Nuclear Weapon System Safety Program (dated 23 December 1996)</i>. This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below. In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether the following four DoD Nuclear Weapon System Safety Standards serve as the foundation of all nuclear weapons safety matters for critical assets include:</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- a. Measures to prevent nuclear weapons designated as critical assets involved in accidents or incidents, or jettisoned weapons, from producing a nuclear yield.
  - b. Measures to prevent nuclear deliberate pre-arming, arming, launching or releasing of nuclear weapons designated as critical assets with the exception of execution of emergency war orders or when directed by competent authority.
  - c. Measures to prevent inadvertent pre-arming, arming, launching, or releasing of nuclear weapons designated as critical assets in all normal and credible abnormal environments.
  - d. Measures to ensure adequate security of nuclear weapons under *DoDD 5210.41*.
2. The assessor must verify whether sufficient Safety Rules are in place to provide the maximum protection possible against the risks and threats to nuclear critical assets.
- ◆ *The following are recommended:*
    - *Nuclear weapons designated as critical assets will not intentionally exposed to an abnormal environment except in an emergency.*
    - *Nuclear weapons designated as critical assets will not be used for training or troubleshooting except as explicitly allowed by a specific safety rule.*
    - *Nuclear weapons designated as critical assets may be used for exercises except when explicitly prohibited by specific safety rules.*
    - *Only certified procedures, personnel, equipment and organizations, authorized by appropriate level of authority will be employed to conduct nuclear weapon system operations.*
    - *Personnel that have physical access to nuclear weapons designated as critical assets will be qualified under the PRP in accordance with DoD Directive 5210.42.*
    - *Nuclear weapons designated as critical assets will be transported in accordance with DoD Directive 4540.5. The following safety procedures will apply:*
      - *Movement will be kept to a minimum consistent with operational requirements.*
      - *Custody and accountability transfers during logistic movements will be by courier receipt system to ensure positive control.*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF NUCLEAR CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>STORAGE DESIGN CRITERIA</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Storage Design Criteria refers to security system design (e.g., physical design, protection criteria, etc.) requirements for nuclear weapons that are designated as critical assets in both non-operational (e.g., depot, site, etc.) storage and operational storage in above ground and in underground site facilities.</p>
<p><b><u>INTENT:</u></b> To ensure that nuclear weapon alert and storage facilities/areas that are designated as critical assets and/or their contents are properly protected and designed to safeguard against the sabotage, theft, loss, seizure or unauthorized access.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Storage Design Criteria will include a review of the requirements associated with the above ground storage and maintenance facilities consisting of area protection system, facility protection system, electronic security systems (ESS), entry and circulation control system, underground storage and maintenance facilities, weapons storage and security systems for critical assets.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Storage Design Criteria of nuclear weapon alert and storage facilities are based on <i>DoD C-5210.41M/Air Force Supplement: Nuclear Weapons Security Manual (dated 1 September 1999)</i>. This reference addresses all the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether sufficient Area Protection System procedures are in place to ensure protection of the nuclear critical asset.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- ◆ *It is recommended that the area protection system consists of the boundary barrier subsystem, the boundary detection subsystem, the boundary detection and assessment subsystem, the area lighting subsystem, the area command and control subsystem and other area protection subsystems for designated nuclear critical assets.*
- ◆ *It is recommended that the perimeter security system for nuclear critical assets provide for positive means of detecting attempted entry, deterring unauthorized entry and providing sufficient delay to the attacking force so that the security force can execute the appropriate response to protect critical assets.*
- ◆ *It is recommended that security lighting be provided for permanent areas to discourage unauthorized entry and create a psychological deterrent to potential intruders for designated nuclear critical assets.*
- ◆ *It is recommended that the site security force be provided a means of controlling site security lighting in and around nuclear critical assets.*
- ◆ *It is recommended that when commercial power is interrupted, emphasis be placed on minimizing the time the perimeter or site illumination is lost with a goal of no lost illumination for designated nuclear critical assets.*
- ◆ *It is recommended that the lighting system, back up power source and any interface equipment be used as a complete system for minimizing lost illumination for nuclear designated critical assets.*
- ◆ *It is recommended that early detection and near real-time assessment be essential for a prompt and effective reaction to any attempt to penetrate the perimeter security system for a designated nuclear critical asset.*
- ◆ *It is recommended that designated nuclear critical asset storage sites and alert areas require redundant and diverse communication systems for site security.*

2. The assessor must verify whether sufficient Facility Protection System procedures are in place to ensure protection of the nuclear critical asset.

- ◆ *It is recommended that the facility protection system for designated nuclear critical assets include the facility barrier system subsystem, the facility detection subsystem, the facility delay and denial subsystem and criteria for support facilities.*
- ◆ *It is recommended that each component of the designated nuclear critical asset storage and maintenance structures be designed to provide equivalent penetration resistance and when combined with other site security measures will aim toward a system goal of 30-minute access delay.*
- ◆ *It is recommended that all permanent facilities used to house nuclear critical assets, permanently or temporarily, have both interior and exterior IDS.*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- ◆ *It is recommended that each land-based storage structure normally used for the storage of designated nuclear critical assets be equipped with systems that delay or deny unauthorized access to and/or removal of a nuclear weapon.*
  - ◆ *It is recommended that planners responsible for the design or modification of a designated nuclear critical asset storage site or alert area consider all aspects necessary to optimize security, safety and efficiency. Facilities to be permanently manned by security forces should be constructed so as to preclude exposure to adverse weather, including temperature extremes.*
3. The assessor must verify whether sensors and associated equipment are included in ESS and as these systems deteriorate and replacement becomes necessary, appropriate upgrades are accomplished.
- ◆ *The following are recommended with regard to IDS:*
    - *IDS will increase the surveillance capability of the security force for designated nuclear critical assets by alerting security personnel to an approach, intrusion or attempted intrusion.*
    - *IDS will provide detection capability in depth for designated nuclear critical assets through the use of detection devices at the perimeter and intrusion detection devices on storage and alert structures.*
    - *IDS for designated nuclear critical assets will safeguard against human or mechanical failure.*
    - *All permanent structures that temporarily or permanently house nuclear critical assets will include both point and motion IDS that are capable of detecting the physical opening of any entry point to an intruder and intruder movement within the structure.*
    - *Control and data transmission media for ESS will be protected commensurate with the level of sensitivity of the information being communicated regarding designated nuclear critical assets.*
4. The assessor must verify whether sufficient Entry and Circulation Control System procedures are in place to ensure the protection of nuclear critical assets.
- ◆ *It is recommended that a system be provided for controlling entry and circulation of authorized personnel and vehicles within the limited and exclusion areas around designated nuclear critical assets.*
  - ◆ *It is recommended that each organization that has a mission or function with designated nuclear critical assets enforce a two-person rule.*
  - ◆ *It is recommended that access Control procedures be established for limited areas surrounding designated nuclear critical assets, to include:*
    - *Controlled picture badge system or entry/authorization roster*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- *Visitor control system*
  - *Duress system*
  - *Inspection or search*
  - ◆ *It is recommended that the entry control facility for the designated nuclear critical asset be part of the area boundary subsystem of the perimeter security system. It should consist of a gatehouse, personnel entry gate, automated entry control portals and a vehicle entrapment area with gates and crash barriers. The facility should be lighted to permit personnel and vehicle identification and inspection in any weather condition. The facility should have a minimum field of view of 180 degrees toward the exterior of the site.*
  - ◆ *It is recommended that the vehicle entry area for designated nuclear critical assets consist of two gates constructed in such a way that when a vehicle enters, the outer gate is opened while the inner gate remains closed. The outer gate will then be closed behind the vehicle before the inner gate is opened to permit the vehicle to enter.*
  - ◆ *It is recommended that the vehicle entry area for designated nuclear critical assets will provide resistance against unauthorized vehicle penetration.*
  - ◆ *It is recommended that all passengers exit the vehicle and proceed through the entry control point as pedestrians.*
5. The assessor must verify whether Underground Storage and Maintenance Facilities are sufficiently secure to ensure protection of nuclear critical assets.
- ◆ *It is recommended that the areas of the underground facility designated for storage and/or maintenance of nuclear munitions that are nuclear critical assets are designated as an exclusion area.*
  - ◆ *It is recommended that the underground portion of the facility designated as a critical asset is bounded by walls and beginning at a designated gate/barrier at either end of the entry/exit tunnel is designated as a limited area.*
  - ◆ *It is recommended that positive entry control procedures be established for entry to underground storage and maintenance facilities for designated nuclear critical assets.*
6. The assessor must verify whether sufficient Weapon Storage and Security System (WS3) procedures are in place and followed to ensure the protection of nuclear critical assets.
- ◆ *The use of the Air Force Weapon Storage and Security System is recommended. It is approved for the storage of designated nuclear critical assets, is a stand-alone system and compensates for many weapon storage requirements. Each WS3 consists of four subsystems/groups. These include a weapons storage vault (WSV), a coder transfer group, a monitor indicator group and a console group.*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- ◆ *It is recommended that the WS3 have an emergency backup opening system that will be protected and controlled.*
- ◆ *It is recommended that the universal unlock codes are stored in approved storage containers within the base/unit command post under U.S. control.*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF NUCLEAR CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>SECURITY FORCE OPERATIONS (SFO)</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Security Force Operations (SFO) refers to the planning, training and tactical deployment of security forces capable of repelling an adversary force intent on damaging, destroying or stealing nuclear resources or material that are designated as critical assets. Sound planning, training, equipping and use of security forces is important in ensuring that this force is capable of repelling an adversary force.</p>
<p><b><u>INTENT:</u></b> To ensure that the principles, tactics and procedures used by the Security Force are sound and capable of repelling an adversary force intent on damaging, destroying or stealing a designated nuclear critical asset.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of SFO will include an assessment of the requirements for security and support forces designated to protect and identify required capabilities of designated nuclear critical assets. It includes requirements for training the tactical preparation of areas, tactical deployment and control of security forces, tactically significant physical security features, initial engagement, phased deployment and employment of weapons.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of SFO are based on <i>DoD C-5210.41-M/Air Force Supplement: Nuclear Weapons Security Manual (dated 1 September 1999)</i>. This reference addresses all the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether there are sufficient forces assigned and designated to provide security for designated nuclear critical assets.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- ◆ *It is recommended that security forces are organized, trained, manned and equipped to provide normal day-to-day protection for designated nuclear critical assets and to react to security incidents involving these critical assets. When warranted by emergency conditions, the primary efforts of security forces should be directed to protect areas in which the critical assets are located and to assure that authorized emergency evacuation or destruction, as applicable, can be accomplished.*
  - ◆ *It is recommended that as a peacetime baseline, security forces will consist of a sufficient number of security forces to control entry into limited and exclusion areas for designated nuclear critical assets and to preclude unauthorized access.*
  - ◆ *It is recommended the security force includes:*
    - *An Area Supervisor (AS) who will direct and manage the area security operation in support of the critical assets and will monitor the well being of forces posted in the area.*
    - *Alarm Monitors (AM) who will monitor IDS dispatch security forces to alarms and make initial notifications for the protection of the critical assets.*
    - *Entry Controllers (EC) who will apply controls that ensure only authorized personnel are admitted to restricted areas for the critical assets.*
    - *Mobile sentries and elevated observers, who may be more effective than Boundary Sentries (BS) in satisfying surveillance requirements for the critical assets, will be armed at all times and will be posted inside or outside the restricted area boundary barrier.*
    - *Response Forces (RF) will be organized and trained as tactical elements, or as a combined force, for those situations, which threaten or affect the security of nuclear weapons designated as critical assets.*
    - *One or more Backup Force (BF) will be organized and trained as tactical elements, or as a combined force, capable of reacting when the RF has been deployed to respond to situations that affect or threaten the security of nuclear weapons designated as critical assets.*
    - *Plans will be maintained for the reinforcement of the RF and the BF during emergencies involving the security of the critical assets.*
2. The assessor must verify whether sentries on post are armed and precautionary actions, including the posting of additional sentries, are taken when warranted.
3. The assessor must verify whether security response force reaction times for the protection of designated nuclear critical assets are sufficient.
- ◆ *It is recommended that security response force reaction times for the protection of designated nuclear assets are as follows:*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- *The RF will deploy in less than the time required for an unopposed individual or a hostile group to effect a penetration and gain unauthorized access to the critical asset. Elements of the reaction force will be capable of responding immediately.*
  - *The BF will be deployed in sufficient time to ensure retention of custody and control of the critical asset or arrival of the AF. The BF will be capable of responding within the amount of time required to penetrate the area boundary and/or facility delay/denial subsystems and gain access to the critical asset.*
  - *The required reaction time for the AF will be in the range of one to four hours depending on the type of weapon, storage configuration, and security systems for the critical assets.*
4. The assessor must verify whether security patrols inspect all areas of possible concealment in and around designated nuclear critical assets for indications of the use of such areas for observation and surveillance of site operations by unauthorized personnel. The perimeter will be randomly checked for site integrity.
- ◆ *It is recommended that security patrols include the random inspection of perimeter for site integrity.*
  - ◆ *It is recommended that security forces assigned to protect designated nuclear critical assets use the degree of force necessary, including deadly force, to prevent damage, loss, theft, sabotage or compromise of the critical asset.*
  - ◆ *It is recommended that the landing of an unannounced aircraft at a designated nuclear critical asset storage site or alert area will result in the immediate response of the RF. In the event an unannounced aircraft lands adjacent to the critical asset storage site or alert area, the BF will be alerted and prepared to respond to the site.*
  - ◆ *It is recommended that communication disciplines be enforced for all radio and or landline transmissions regarding the status or protection of designated nuclear critical assets on the security force communication net(s).*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF NUCLEAR CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>TRAINING</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Nuclear Security Training refers to the training and exercise program designed to assure the attainment and maintenance of the critical asset staff's and security forces' capability to protect nuclear weapons, nuclear weapon systems, and nuclear components that are designated as critical assets from unauthorized access, damage or sabotage, unauthorized destruction, loss of custody, capture or theft and unauthorized use during all phases of their life cycle.</p>
<p><b><u>INTENT:</u></b> To ensure that the critical asset staff and security force personnel involved in the protection of nuclear critical assets receive the basic and specialized training necessary to attain the skills they need to apply the security techniques required. Critical asset staff and security force personnel will be trained so that they are capable of early detection and apprehension of intruders, preferably before the intruders have completely penetrated the area perimeter.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Nuclear Security Training program for critical asset personnel and security forces will include general security training, transportation security training and security supervisory personnel training. The assessment will also include any specialized training pertaining to specific duties assigned and duty location, training exercises and a review of training records maintained for each individual.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Training are based on <i>DoD- 5210.41-M/Air Force Supplement: Nuclear Weapons Security Manual (dated 1 September 1999)</i>. This reference addresses all the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether local exercises involving the security force protecting designated nuclear critical assets are being conducted as frequently as needed to maintain a high degree of readiness.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

2. The assessor must verify whether sufficient training and quality control program for security forces assigned to protect designated nuclear critical assets.
  - ◆ *It is recommended that the following areas are incorporated into training and quality control programs for security forces assigned to protect designated nuclear critical assets:*
    - *Adversary groups, their motivation and objectives, tactics and recognition of sabotage-related devices and equipment*
    - *Individual and small unit day and night tactics, to include fire control, cover and concealment and fire and maneuver*
    - *Use of standard military night vision equipment to include thermal imagers and weapon sights for maximum nighttime effectiveness*
    - *Interaction with other units, fire and maneuver, command and control, actions at the objective and communications outages*
    - *Guidance will include standard operating procedures, coordination of fire between units, actions at the objective, motivation of forces, clear plan of succession and command and control, with and without communications.*
    - *Supervisory initiative at the onset of hostilities*
    - *Thorough debriefs after exercises to prevent repetition of mistakes*
    - *Defense against standoff attack*
    - *Site defense plan*
    - *Airborne threat engagement*
    - *Inspections, to include individuals, vehicles and hand-carried items*
3. The assessor must verify whether inspections simulating normal and increased threat conditions are performed to determine how prepared the security forces are to secure the protection of designated nuclear critical assets.
4. The assessor must verify whether security force personnel assigned to duties involving the protection of designated nuclear critical assets are sufficiently trained.
  - ◆ *It is recommended that security force personnel assigned to duties involving the protection of designated nuclear assets be trained in the subjects listed below. Personnel designated to augment or reinforce security forces in emergencies should also be trained in these subjects commensurate with their planned participation in security force emergency operations.*
    - *General training*
    - *Security skills training*

**For Official Use Only**  
**Draft CIP FSVA Nuclear Security Standards**

- *Transportation security training*
- *Security supervisory personnel training*
- ◆ *It is recommended force-on-force training be provided every 18 months for security forces at all locations where designated nuclear critical assets are stored or deployed.*
- ◆ *It is recommended that training records be maintained on each individual assigned to the security force.*

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

**SECURITY OF CHEMICAL CRITICAL ASSETS**

**DESCRIPTION:**

Chemical Security Standards covers the security measures and actions designed to safeguard chemical agents located in facilities that house critical assets and to increase the security of a facility/site containing critical assets to include storage, security force operations, personnel reliability, training, safety and material control and handling procedures.

<b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF CHEMICAL CRITICAL ASSETS</i>
<b><u>TOPIC:</u></b> <i>PERSONNEL RELIABILITY</i>
<b><u>SUBTOPIC:</u></b> <i>PERSONNEL RELIABILITY PROGRAM (PRP)</i>
<b><u>EXPLANATION:</u></b> Personnel Reliability Program (PRP) refers to the process of granting or denying individual access to sensitive information, equipment or materials that are associated with the critical asset based on investigations and verification of individual trustworthiness and loyalty.
<b><u>INTENT:</u></b> To ensure that access to restricted information, equipment or materials associated with a critical asset is limited to those personnel who require access and for whom investigations verifying their trustworthiness and loyalty have been completed.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the PRP will include a review of the policies, responsibilities, procedures for management and standards of individual reliability in personnel performing duties associated with chemical agents and their components. Additionally, an assessment will be performed on the processes for the selection and retention of personnel. An assessment will also be made of the administration of the day-to-day functions of the PRP to include monitoring of the program, the dissemination of PRP information, the reviewing and certifying officials, supporting staffs, indoctrination and training and administrators on program objectives and procedures.

## For Official Use Only

### Draft CIP FSVA Chemical Security Standards

#### **CRITERIA:**

The standards for the assessment of PRP are based on guidelines contained in *Army Regulation (AR) 50-6: Chemical Surety (dated 26 June 2001)* and *Department of Defense Directive (DoDD) 5210.65: Chemical Agent Security Program (dated 15 October 1986)*. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether responsible officials of sites, arsenals, depots and other organizations responsible for surety programs have appointed surety officers with duties as prescribed in *AR 50-6*.
2. The assessor must verify whether responsible officials having custody of chemical agents have implemented a PRP.
  - ◆ *It is recommended that individuals certified into the PRP will be under continuing evaluation to ensure adherence to safety, security and reliability standards. Individuals who do not meet or maintain program standards will not be selected for or retained in the PRP or assigned chemical agent protection duties.*
3. The assessor must verify whether responsible officials have designated an official to certify individuals' suitability for the PRP.
  - ◆ *It is recommended that the certifying official will be in a supervisory role and will be responsible for performing the assigned chemical agent mission. In large organizations where the designated official may not have close personal contact with all the personnel, it is recommended that he or she may delegate the duties of the certifying official.*
  - ◆ *It is recommended that certifying officials will be personnel authorized to perform this function. Contractor personnel will be prohibited from acting as certifying officials.*
  - ◆ *It is recommended that no one will be assigned to a PRP position until the certifying official screens and certifies the individual as suitable for the PRP. Before the certifying official assumes duties, the reviewing official will screen and certify the certifying official into the PRP.*
  - ◆ *It is recommended that for Government-Owned, Contractor-Operated (GOCO) and Contractor-Owned, Contractor-Operated (COCO) facilities with chemical agent missions, the responsible Contracting Officer's Representative (COR) or properly designated subordinate will serve as the certifying official for DoD contractor employees authorized to perform chemical security duties.*

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

- ◆ *It is recommended that certifying officials appoint PRP monitors to assist in administering the day-to-day functions of the PRP. PRP monitors will also be appointed at sites or activity level to administer the consolidated day-to-day functions of multiple certifying officials.*
4. The assessor must verify whether changes in the PRP assignment status of personnel are reported per AR 600-8-11, AR 600-8-23, AR 600-8-104, AR 680-29, and *Department of the Army Pamphlet (DA Pam) 600-8-23*.
  5. The assessor must verify whether certifying officials have identified each position required to accomplish chemical security duties.
    - ◆ *It is recommended that each organization or activity assigned a chemical agent mission and required to implement a PRP will establish and maintain a Chemical Duty Position Roster (CDPR).*
    - ◆ *It is recommended that certifying officials will delete from the CDPR individuals who are administratively terminated or permanently disqualified. Each certifying official will maintain a CDPR.*
  6. The assessor must verify whether prior to authorizing an individual to perform chemical duties, the certifying official has ensured that any required formal instruction is completed and/or the individual has the requisite experience applicable to the PRP position assigned and is proficient in assigned chemical duties.
  7. The assessor must verify whether personnel whose regularly assigned duties involve access to or security of chemical agents are screened initially for suitability and reliability.
    - ◆ *It is recommended that these personnel be evaluated on a continuing basis at the supervisory level to ensure that they continue to meet the high standards required.*
  8. The assessor must verify whether all PRP personnel have had a favorable National Agency Check (NAC) completed within the last 5 years before initial assignment.
  9. The assessor must verify whether PRP personnel have been re-screened every 5 years unless rescreening occurs sooner.
    - ◆ *It is recommended that a new investigation be required when there has been an intervening assignment to a non-chemical duty position.*

**For Official Use Only**  
**Draft CIP FSV A Chemical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF CHEMICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>FACILITY SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Chemical Facility Security refers to system and procedures established to prevent the loss, theft, unauthorized access and use, sabotage or destruction of chemical agents, facilities or components that are designated as critical assets.</p>
<p><b><u>INTENT:</u></b> Chemical security measures for facilities will ensure that the chemical agents, facilities or components that are designated as critical assets will not be subject to loss, theft, sabotage, unauthorized use, unauthorized destruction, unauthorized disablement or accidental damage.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Chemical Facility Security measures will include assessing the measures designed to safeguard and protect the critical asset from access by unauthorized individuals or potential adversaries. This will include examining the overall security posture of the facility by reviewing the security plans and procedures that are in place, assessing the effectiveness of the security force protecting the facility, the use of physical features outside and within the perimeter of the facility and the technical devices or other security measures that impede or hinder a potential intruders or adversaries from gaining access to the critical assets.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Chemical Facility Security are based on <i>AR 190-59: Chemical Agent Security Program (dated 1 July 1998)</i>. This reference addresses all the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether only authorized personnel are permitted entry into limited and exclusion areas where critical assets are housed.<ul style="list-style-type: none"><li>◆ <i>It is recommended that control procedures assure positive identification of all personnel prior to entry.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

2. The assessor must verify whether security patrols inspect all areas of possible concealment in and around the critical asset for indications of the use of these areas for observation and surveillance of critical assets by unauthorized personnel.
  - ◆ *It is recommended that checks will be made using random routes at least once daily. This check should include the facility perimeter that will be randomly checked for site integrity (e.g., no breaks in the fence, no evidence of attempted penetrations, etc.).*
3. The assessor must verify whether exterior inspections of all structures containing critical assets are conducted for signs of tampering and covert entry
  - ◆ *It is recommended that the results of the inspection be annotated in the guard force log or other suitable form.*
4. The assessor must verify whether doors used for main access to chemical agent storage structures containing critical assets are sufficiently locked to ensure sufficient protection of chemical critical assets.
  - ◆ *It is recommended that doors used for main access to chemical storage structures containing critical assets are locked with two high security locks. Each high security lock should be mounted on a high security shrouded hasp. It is recommended that all doors and openings in excess of 96 square inches are equipped with IDS coverage.*
5. The assessor must verify whether perimeter gates, vents, grills and gratings are locked with low-security padlocks.
  - ◆ *It is recommended that hasps that are mounted on gates, vents, grills and gratings provide protection from forced entry equal to the lock.*
6. The assessor must verify whether the limited area surrounding chemical agent storage structures designated as critical assets are sufficiently protected.
  - ◆ *It is recommended that these areas are protected by two perimeter fences separated not less than 30 feet, no more than 150 feet.*
  - ◆ *It is recommended that a steel cable of sufficient strength to impede vehicular penetration be installed outside the outer fence in which topography permits high-speed approach.*
7. The assessor must verify whether drainage structures, water passages and other openings penetrating the perimeter fence are barred to prevent access to critical assets.
8. The assessor must verify whether fence lines around critical assets are sufficient to protect chemical critical assets.
  - ◆ *It is recommended that fence lines around critical assets have 30-foot clear zone outside the outer fence. The entire zone between the outer and inner fences and the area inside the inner fence should also be cleared.*

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

9. The assessor must verify whether perimeter lighting around critical assets is positioned and designed to enable the detection of persons in the entire clear zone, inside the inner perimeter fence, between the fences and outside the outer perimeter fence.
10. The assessor must verify whether lighting fixtures around critical assets are positioned to avoid the blinding or silhouetting guards.

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF CHEMICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>SAFETY AND OCCUPATIONAL HEALTH</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Safety and Occupational Health refers to the special safety considerations involving chemical agent, personnel and procedures associated with a critical asset that contributes to the security and safety as well as providing maximum protection to workers, the environment and surrounding communities, consistent with operational requirements.</p>
<p><b><u>INTENT:</u></b> To ensure that the standards governing chemical critical assets safety and occupational health provide the maximum protection possible against the risks and threats inherent in today's environment to personnel, the general environment and surrounding communities.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Safety and Occupational Health will consist of a review of the responsibilities and procedures to ensure chemical agents are properly safeguarded to ensure the health and safety of employees associated with the critical asset. A chemical event encompasses chemical accidents, incidents and other circumstances where there is a confirmed or likely release to the environment, exposure of personnel, threat to the security of chemical agent materiel or any incident of concern to the local authorities.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of the Safety and Occupational Health are based on <i>AR 50-6: Chemical Security (dated 26 June 2001)</i>. This reference addresses all the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether an occupational health program has been established in support of the chemical surety program per <i>AR 11-34</i> and <i>AR 401-5</i></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

2. The assessor must verify whether security forces that respond to chemical events are made aware of chemical agent categories and/or classifications.
3. The assessor must verify whether chemical agent research and development contractors report chemical events (e.g., chemical release to the environment, exposure of personnel, threat to the security of chemical agent materiel, etc.) as specified in their contract.
4. The assessor must verify whether responsible officials report any chemical event that is declared a community emergency by the most efficient means available to the State and local emergency response officials responsible for the affected areas and notify these officials of all levels of emergency as coordinated and established in local plans and agreements.
  - ◆ *It is recommended that chemical sites/activities report chemical event situations to the public per local agreements; however, loss of chemical agent and criminal or terrorist acts directed at chemical munitions, agents or storage areas will not be reported without appropriate authorities' approval.*
  - ◆ *It is recommended that Prior to a news release to the public, the State and local government officials, to include the local congressional office, will be notified of a chemical event, if at all possible. In cases where health and safety reasons preclude prior congressional notification, the news release and local congressional notification may occur simultaneously.*
  - ◆ *It is recommended that for release of chemical agents that presents a hazard to the public or occurs outside of a government critical asset, specific guidelines in AR 360-5 will apply.*
  - ◆ *It is recommended that for chemical events occurring at facilities housing critical assets, the responsible authority will coordinate all news media releases with the responsible officials per local procedures.*
5. The assessor must verify whether chemical events that meet the criteria for Class A or B accidents or involve release of a chemical agent outside the boundaries of government reservations, excluding COCO facilities, are investigated.
6. The assessor must verify whether procedures have been established to review each chemical event and to initiate safety investigations when warranted.
  - ◆ *It is recommended that a responsible official direct or request a local investigation of a chemical event by an investigating party or investigating board.*
7. The assessor must verify whether safety procedures and guidance for the use and handling of Research, Development, Test, and Evaluation (RDT&E) of chemical solutions are followed as outlined in AR 385-61 and DA Pam 385-61.

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

- ◆ *It is recommended that responsible officials implement a Chemical Agent Safety Program.*
8. The assessor must verify whether responsible officials apply Occupational Safety and Health Administration (OSHA) and other non-military regulatory or consensus safety and health standards to chemical agents, chemical agent derivatives, equipment, systems, operations or workplaces containing chemical agents as practicable.
  9. The assessor must verify whether a hazard analysis has been conducted for each chemical operation to include Recovered Chemical Warfare Material (RCWM), research chemical agents and toxic chemical agents and munitions.
  10. The assessor must verify whether plans and procedures are in place to respond to leaking chemical munitions or containers in storage.
  11. The assessor must verify whether procedures for RCWM are in place and followed to ensure protection of chemical critical assets.
    - ◆ *The following are recommended:*
      - *Safety concerning RCWM containing suspect chemical agents will be per AR 50-6, Chapter 8.*
      - *Safety concerning RCWM containing suspect highly toxic industrial chemicals (e.g., chlorine, hydrogen cyanide, potassium cyanide, etc.) will be per AR 385-10 and practices which are generally accepted for industrial operations.*
      - *Safety concerning RCWM containing explosive components will be per AR 385-61, AR 385-64, DA Pam 385-61 and DA Pam 385-64.*
  12. The assessor must verify whether security concerning RCWM containing suspect chemical agent or explosives meets the protective measures specified in AR 190-11 for Category II ammunition and explosives.
    - ◆ *The following is recommended:*
      - *Vulnerability assessments should be used to modify protective measures subject to approval by the responsible authority in the chain of supervision of the operation.*
      - *Outside of material located on an installation with a chemical surety mission, access to such items should be limited to Explosive Ordnance Disposal (EOD) or Technical Escort Unit (TEU) personnel who are knowledgeable concerning the safety, security, custody and accountability of chemical agents and explosives. Although these personnel are not required to be in the PRP, the two-person rule applies for reasons of safety.*
  13. The assessor must verify whether approved safety and health plans and procedures are currently required for RCWM sites.

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF CHEMICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>STORAGE DESIGN CRITERIA</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Safety and Occupational Health refers to the special safety considerations involving chemical agent, personnel and procedures associated with a critical asset that contributes to the security and safety as well as providing maximum protection to workers, the environment and surrounding communities, consistent with operational requirements.</p>
<p><b><u>INTENT:</u></b> To ensure that the chemical storage sites for critical assets are properly constructed, secured and prevent the unauthorized access of individuals and potential adversaries from gaining access to chemical critical asset storage sites.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Storage Design Criteria for chemical critical assets will include a review of the security measures associated with how the agents are being stored. The assessment will include storage structure walls, ceilings, roofs, door hinges, windows, locking systems, IDS, and the requirements associated with the category of chemical agents being stored.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Storage Design Criteria are based on guidelines contained in <i>AR 190-59: Chemical Agent Security Program (dated 1 July 1998)</i> and <i>Defense Threat Reduction Agency (DTRA) Antiterrorism Vulnerability Assessment Team Guidelines (dated October 2001)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this topic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether storage sites for chemical agents are as small as possible and consolidated consistent with operational planning and safety factors.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

- ◆ *It is recommended that chemical agents not be co-located in storage structures with unrelated material. Chemical agents should be stored in enclosed storage structures or as prescribed in AR 190-59. Classified chemical agents should be secured, stored, and transported according to AR 380-5, and DoD 5220.22-R, for contracts, as appropriate.*
- 2. The assessor must verify whether corrective actions are being performed and monitored to ensure security requirements are established and maintained.
- 3. The assessor must verify whether physical security inspections of chemical agent storage facilities, to include chemical demilitarization facilities, are being conducted according to the requirements in AR 190-13, Chapter 2.
- 4. The assessor must verify whether access to chemical agents are being controlled according to the two-person rule requirements in AR 50-6, and appropriate lock and key control procedures have been established to preclude defeat of the two-person rule.
- 5. The assessor must verify whether doors used for main access to storage structures containing chemical agents are locked with two high-security padlocks mounted on a high-security shrouded hasp.
  - ◆ *It is recommended that other doors that are not ordinarily used for access are secured from within and will provide resistance to penetration equivalent to that of the structure itself.*
- 6. The assessor must verify whether all storage structures, buildings, or rooms in which chemical agents are stored are protected with interior IDS to detect the physical opening of any entry point.
- 7. The assessor must verify whether a threat assessment is used as the basis for identifying and prioritizing facility upgrades and developing barrier plans.
  - ◆ *It is recommended that the threat assessment provide a design basis threat for use in planning, programming and designing new construction.*
- 8. The assessor must verify whether the site facility engineer and physical security personnel are being made aware of training courses focusing on incorporating physical security principles and practices into construction.
- 9. The assessor must verify whether appropriate facility engineering and physical security personnel are remaining knowledgeable of the latest construction standards contained in DoD 2000.16.
  - ◆ *It is recommended that the site incorporate the standards in all new construction and renovation projects. These projects should include a physical security review at all stages of planning, programming, design and construction.*

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

10. The assessor must verify whether a review has been performed on all site master plans, design guides and architectural compatibility standards to ensure compatibility with physical security standards, concerns and guidelines.
- ◆ *It is recommended that this review include a prioritized list of threat factors for site selection.*

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF CHEMICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>MATERIAL CONTROL/HANDLING PROCEDURES</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Chemical Material Control/Handling Procedures refers to measures and actions taken to ensure controlled and safe movement of packages, material and vehicles into controlled/restricted areas housing critical assets at the chemical agent site.</p>
<p><b><u>INTENT:</u></b> To ensure that personnel with access to chemical agents that are associated with critical assets adhere to positive searches and inspections for prohibited items and contraband at the critical asset site.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> To ensure that personnel with access to chemical agents that are associated with critical assets adhere to positive searches and inspections for prohibited items and contraband at the critical asset site.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Material Control/Handling Procedures are based on <i>AR 190-59: Chemical Agent Security Program (dated 1 July 1998)</i>. This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether procedures are prescribed to control movement of packages, material and vehicles into and out of chemical agent site limited areas housing critical assets.<ul style="list-style-type: none"><li>◆ <i>It is recommended that searches and inspections for prohibited items and contraband be conducted in accordance with AR 190-22 and AR 190-59.</i></li></ul></li><li>2. The assessor must verify whether responsible officials prescribe procedures to be followed when unauthorized items are found or when an individual refuses to be searched upon probable cause.</li><li>3. The assessor must verify whether inspection procedures sufficiently address hand carried items and all vehicles entering and leaving a secured area.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

- ◆ *It is recommended that upon entering a limited area, all hand-carried items (e.g., handbags, purses, etc.) will be inspected by security personnel for readily detectable prohibited items and contraband. Hand carried items leaving the limited area should be inspected for unauthorized removal of chemical agents at the discretion of the responsible official concerned.*
  - ◆ *It is recommended that upon entering or leaving a limited area, security personnel will inspect all vehicles for unauthorized personnel and readily detectable prohibited and contraband items.*
  - ◆ *It is recommended that only essential emergency and contractor vehicles and materials handling equipment will be permitted to enter limited areas.*
4. The assessor must verify whether vehicles and material handling equipment remaining in limited or exclusion areas after duty hours will be sufficiently secured to assure that they are not readily usable by a hostile force.
- ◆ *It is recommended that no vehicle or material handling equipment is allowed to park within the inner or outer clear zone of the chemical agent site.*
5. The assessor must verify whether signs requiring removal of the ignition keys and locking of all vehicles are placed in all parking areas adjacent to facilities or areas containing chemical agents.
6. The assessor must verify whether responsible officials have established separate standards for the security, parking and removal of ignition keys or immobilization of official security force vehicles.
7. The assessor must verify whether local security procedures in support of Chemical Weapons Treaty inspection mission have been developed and implemented.
- ◆ *It is recommended that these security procedures include measures that will preclude the unauthorized access to security interests and be modified to meet packages and material control standards.*

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF CHEMICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>SECURITY FORCE OPERATIONS (SFO)</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Security Force Operations (SFO) refers to designated persons specifically organized, trained and equipped to provide physical security and perform law enforcement tasks in the safeguarding of chemical agents designated as critical assets and the protection of their storage sites.</p>
<p><b><u>INTENT:</u></b> To ensure that the principles, tactics and procedures used by the Security Force are sound and capable of repelling an adversary force. Sound planning, training, equipping and use of security forces is important in ensuring that this force is capable of repelling an adversary force.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of SFO will include the physical security requirements outlined in the site security plan and in applicable regulations. The programs and efforts that go into the development, evaluation and revision of the site security plan will address the specific and anticipated localized threat including threat detection, delay, identification, assessment, response, recovery and other measures necessary to protect the critical assets. The provisions of these standards will be applicable to all Category I or II chemical agent storage sites.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of SFO are based on guidelines contained in <i>AR 190-59: Chemical Agent Security Program (dated 1 July 1998)</i> and <i>DoDD 5210.65 (dated 15 October 1986)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this topic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether appropriate CW detection and Personnel Protection Equipment (PPE) has been provided to security forces.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

- ◆ *It is recommended that forces hand carry PPE when on patrol in able to afford protection to the site in the case of agent release (whether accidental or terrorist release) and to assist in the recovery of agents in the event of their loss.*
- 2. The assessor must verify whether there are sufficient security forces assigned and designated in the site security plan to satisfy the necessary security requirements for the site.
  - ◆ *It is recommended that security forces are organized, trained, manned and equipped to provide normal day-to-day protection for chemical agents and to react to security incidents involving chemical agents.*
- 3. The assessor must verify whether responsible officials ensure that only qualified personnel are used to safeguard chemical agents, and take necessary actions to ensure that security force personnel who do not meet Personnel Reliability Program (PRP) requirements are not assigned to protect chemical storage sites.
  - ◆ *It is recommended that standards in AR 190-56 be applicable to civilian security guards assigned to chemical agent security duties.*
- 4. The assessor must verify whether security force sentries on post are forbidden to use of recreational materials.
- 5. The assessor must verify whether security force personnel tasking is appropriate.
  - ◆ *It is recommended that security force personnel not be tasked to perform any functions other than security functions while on duty. Responsible officials should monitor and evaluate overtime hours and take appropriate action to preclude excessive overtime by security force guards.*
- 6. The assessor must verify whether written orders/directions covering site security are being provided for each guard post and security force patrol.
  - ◆ *It is recommended that orders will either be carried by the security forces or be available for use at the site. The orders should include instructions on the use of force.*
- 7. The assessor must verify whether responsible officials ensure there are sufficiently trained security force guards to control entry and to prevent unauthorized access to sites containing chemical agents.
  - ◆ *It is recommended that security forces consist of a Backup Force (BF), Reaction Force (RF) and Alert Force (AF).*
  - ◆ *It is recommended that a portion of the storage site RF is deployed in a random manner in either fixed observation or fighting positions and as mobile foot or vehicle patrols. Posted security force sentries should not be a part of the RF numerical requirement and will continue their assigned tasks when the RF is deployed.*

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

8. The assessor must verify whether the RF conducts training exercises to maintain proficiency.
9. The assessor must verify whether the security force is equipped and armed for combat type operations.
  - ◆ *It is recommended that the vulnerability assessment and local surrounding environment be considered in determining the types of weapons to be employed at the chemical agent storage site.*
10. The assessor must verify whether tactical defense planning has been included in the chemical agent site defense plan.
  - ◆ *It is recommended that preplanned weapons fire is set up for the final defense of the storage facility.*
11. The assessor must verify whether security patrols conduct searches in all areas of possible concealment around the site for indications of the use of such areas for observations and surveillance of site operations by unauthorized personnel.
  - ◆ *It is recommended that security logs be maintained by the security force to record the chronology of events during a shift.*
12. The assessor must verify whether security forces have the ability to control entry and to prevent unauthorized access to facilities/sites containing chemical agents.
  - ◆ *It is recommended that backup forces capable of responding to attempted penetrations and preventing unauthorized removal of chemical agents are in place at all chemical agent storage sites 24 hours a day.*
13. The assessor must verify whether security force members are provided appropriate, realistic site defense force training exercises.
  - ◆ *It is recommended that the training be tailored to each storage site based on the threat and the Vulnerability Assessment (VA) conducted at the site.*
14. The assessor must verify whether site security forces develop plans for the recovery of chemical agents/munitions in the event of their loss.

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF CHEMICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>TRAINING</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Chemical Security Training refers to the training and exercise program designed to assure the attainment and maintenance of the critical asset staff's and security forces' capability to protect chemical critical assets from unauthorized access, damage or sabotage, unauthorized destruction, loss of custody, capture or theft and unauthorized use during all phases of its life cycle.</p>
<p><b><u>INTENT:</u></b> To ensure that the critical asset security force personnel involved in the protection of biological critical assets receive the basic and specialized training necessary to attain the skills they need to apply the security techniques required. Critical asset staff and security force personnel will be trained so that they are capable of early detection and apprehension of intruders, preferably before the intruders have completely penetrated the area perimeter.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Chemical Security Training program for critical asset personnel and security forces will include general security training, transportation security training and security supervisory personnel training. The assessment will also include any specialized training pertaining to specific duties assigned and duty location, training exercises and a review of training records maintained for each individual.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Training are based on guidelines contained in <i>AR 190-59: Chemical Agent Security Program (dated 1 July 1998)</i>. This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. Responsible officials will establish a basic security training program to support the specific security needs of the critical asset.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Chemical Security Standards**

- ◆ *It is recommended that the security program include general training, security skills training, transportation security and security supervisory personnel training.*
- 2. Security force personnel will receive specialized training, certified by a supervisor, pertaining to their specific duties and duty location.
  - ◆ *It is recommended that training include specific information of agents, symptoms, detection devices and capabilities and protective actions to include Personal Protection Equipment (PPE) such as mask fitting, testing and donning procedures.*
- 3. The assessor must verify whether responsible officials have establish a continuing training/education program to ensure all security force personnel and critical asset staff are able to perform routine duties competently and to meet emergencies quickly and efficiently.
- 4. The assessor must verify whether training records are being maintained on each individual assigned to the critical asset site.
- 5. The assessor must verify whether force-on-force training exercises are being conducted to improve and maintain the proficiency of responding site security forces.
- 6. The assessor must verify whether security force personnel are receiving training to ensure they are thoroughly knowledgeable of the weapons with which they are armed, to include the proper care, maintenance, safety features, malfunctioning and corrective actions and are cross-trained and familiar with all weapons available to the security force.
- 7. The assessor must verify whether designated authorities prescribe the frequency of training in live fire of weapons to ensure acceptable levels of weapon proficiency are developed for security forces armed with such weapons.
  - ◆ *It is recommended that requirements in DA Pam 350-38 and AR 190-56 be used as guidance.*
- 8. The assessor must verify whether responsible officials have determined the adequacy of the security training program through periodic evaluation of the critical asset staff and security force proficiency during response exercises conducted under a variety of different conditions.
- 9. The assessor must verify whether Fire, Emergency Medical Services (EMS) and Hazardous Material (HAZMAT) training complies with applicable requirements of 29 CFR 1910.120, National Fire Protection Association (NFPA) 472 and 473 and the local, State, Federal or host-nation regulations governing emergency medical services care.

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

**SECURITY OF BIOLOGICAL CRITICAL ASSETS**

**DESCRIPTIONS:**

Security of Biological Critical Assets refers to measures and actions carried out to increase the security of a biological facility and/or material that is designated as a critical asset. An assessment of a biological critical asset may include any of the following components: personnel reliability, facility security, safety, storage, material control and handling, security force operations and training.

<b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF BIOLOGICAL CRITICAL ASSETS</i>
<b><u>TOPIC:</u></b> <i>PERSONNEL RELIABILITY</i>
<b><u>SUBTOPIC:</u></b> <i>PERSONNEL RELIABILITY PROGRAM (PRP)</i>
<b><u>EXPLANATION:</u></b> Personnel Reliability Program (PRP) refers to the process of granting or denying individual access to sensitive information, equipment or materials that are associated with a critical asset based on investigations and verification of individual trustworthiness and loyalty.
<b><u>INTENT:</u></b> To ensure that access to restricted information, equipment or materials associated with a biological critical asset is limited to those personnel who require access and for whom investigations verifying their trustworthiness and loyalty have been completed.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the PRP will include a review of all scientific, support and protective personnel working within a biological facility designated as a critical asset, including the identification of personnel reliability positions, to ensure they maintain proper clearance status under all applicable PRP. Additionally, assessments will include a review of the screening process, training and records.

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

**CRITERIA:**

The standards for the assessment of the PRP are based on guidance contained in *Army Regulation (AR) 190-XX: Biological Security (Draft) (undated)* and in *42 CFR Part 73, 7 CFR Part 131* and *9 CFR Part 121 (date unknown)*, which provide Federal standards governing the storage, handling and use of biological agents listed as “select” by the Center for Disease Control (CDC). The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether positions requiring personnel reliability screening and clearance have been identified in organizational personnel requirements documents.
2. The assessor must verify whether all individuals assigned to positions requiring personnel reliability screening have completed screening in accordance with the referenced documents.
3. The assessor must verify whether personnel reliability screening procedures for personnel working with biological agents are being performed in accordance with guidance contained in the referenced documents.
4. The assessor must verify whether personnel security risk assessments are being updated every 5 years.
5. The assessor must verify whether the responsible authority has established an after-hours access list that specifies those individuals cleared for after hours access, either escorted or unescorted.
  - ◆ It is recommended that the access roster include the identity of those employees granted access and the specific facilities or areas to which individual access is authorized.

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF BIOLOGICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>BIOLOGICAL FACILITY SECURITY</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Biological Facility Security refers to the system and procedures established to prevent the loss, theft, unauthorized access and use, sabotage or destruction of biological critical assets.</p>
<p><b><u>INTENT:</u></b> Biological security measures for facilities will ensure that the biological agents, facilities or components designated as critical assets will not be subject to loss, theft, sabotage, unauthorized use, unauthorized destruction, unauthorized disablement or accidental damage.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Biological Facility Security will involve all procedures, systems and plans in place to protect a biological facility and the critical materials located within it or during transportation. The assessment will ensure the facility is in compliance with the Federal regulations governing a biological facility. External barriers and protective structural features will be assessed. In addition, access to restricted areas and the systems and procedures in place to prevent unauthorized access to restricted areas will be assessed.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Facility Security are based on guidelines contained in <i>42 CFR Part 73</i>, <i>7 CFR Part 131</i>, and <i>9 CFR 121 (undated)</i>, and <i>AR 190-XX: Biological Security (Draft)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this topic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether the facility maintains and adheres to a Site Security/Physical Security Plan.<ul style="list-style-type: none"><li>◆ <i>The following are recommended with regard to this plan:</i><ul style="list-style-type: none"><li>➤ <i>Each facility approved to use, hold or transfer any etiologic materials designated as select agents will develop and implement a security plan establishing policies</i></li></ul></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

*and procedures that ensure the security of the restricted areas containing the select agents. The physical security plan will clearly define threats, examine vulnerabilities and mitigate risks.*

- *The plan will include provisions for controlling, securing, accounting for and limiting access to select agents or sensitive materials.*
  - *The responsible official will review the security plan annually and after any incident.*
  - *The physical security plan will also meet the provisions of AR 190-13, which provides requirements to be considered when developing physical security programs. These requirements include planning for security during peacetime, mobilization, wartime and contingency operations.*
2. The assessor must verify whether sufficient procedures for Facility Certification have been established and adhered to.
- ◆ *It is recommended that facilities that use, hold, or transfer any etiologic materials designated as select agents by the CDC or Animal Plant Health Inspection Service (APHIS) be registered and have applicable authorization by the Department of Health and Human Services or the Department of Agriculture.*
3. The assessor must verify whether sufficient procedures for Access Control have been established and adhered to.
- ◆ *It is recommended that unescorted access to restricted areas is allowed only to individuals passing the risk assessment detailed in 42 CFR 73 and performing a specifically authorized function at an authorized time. Individuals, not approved under Part 73, should be escorted by cleared personnel at all times when in restricted areas.*
4. The assessor must verify whether sufficient procedures for Two-Person Control have been established and adhered to.
- ◆ *The following are recommended with regard to Two-Person Control:*
    - *Access to high-priority restricted areas containing certain etiologic agents or sensitive materials will be controlled according to the two-person access rule.*
    - *The two-person rule will be implemented for work conducted with select agents. This rule also may be accomplished through the use of video monitoring, roving patrols or a combination of means. Personnel will be familiar with safety and security requirements.*
5. The assessor must verify whether sufficient procedures for Periodic Inspections have been established and adhered to.
- ◆ *It is recommended that physical security inspections of biological facilities be conducted according to requirements in DoD 5210.6X and AR 190-13, Chapter 2.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

*All facilities should be inspected annually. Physical security inspections should also be conducted for new biological storage or Research Development Testing and Evaluation (RDT&E) facilities before and immediately after occupancy, on significant change in facility structure, after any forced entry or attempted forced entry with or without theft, and when activities have received an unsatisfactory rating on an external physical security inspection.*

6. The assessor must verify whether responsible officials are developing specific and validated threat assessments.
7. The assessor must verify whether the use of barriers is sufficient in the protection of critical biological assets.
  - ◆ *The following are recommended with regard to the use of barriers:*
    - *Physical barriers will provide physical security measures to properly safeguard against loss, theft, sabotage, diversion or unauthorized use or access to biological agents or sensitive materials designated as critical assets.*
    - *Biological critical asset facilities will have at least one perimeter fence, immediately surrounding the facility. The perimeter fence will be located, with due consideration to required clear zones, terrain features, property lines, and building layouts, not less than 30 feet nor more than 150 feet from buildings or objects being protected. The fence will meet the standards and specifications described in U.S. Army Corps of Engineers (USACE) Standard Design Drawing (SDD) 872-90-04 for non-censored fence and/or 872-90-05 for censored fence and have a seven feet high fabric plus outriggers. Terrain under the fence will be made resistant to erosion or other physical forces that may help facilitate unauthorized penetration of perimeter security.*
    - *The following security construction standards will apply to rooms and laboratories containing select agents or sensitive materials.*
      - *Walls, floors and ceilings will be constructed of at least ½-inch plywood or one-inch tongue-in-groove wallboards or the equivalent. Roofs with suspended ceilings will be protected to ensure the crawl space cannot be used for covert entry.*
      - *Windows and openings (e.g., conduits, vents ducts, etc.) in excess of 96 square inches with a smallest dimension greater than six inches will be barred or grilled to ensure a degree of security comparable to that provided by the walls of the room or laboratory.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- *Doors will be constructed of solid core wood or metal, possess the appropriate Underwriters Laboratory (UL) fire rating and be designed to complement the security provided by the exterior walls of the rooms or laboratories. Hinges will be mounted inside the room or laboratory or if this is not possible, hinges mounted outside such rooms or laboratories will be welded or brazed to preclude removal from outside the door. Doors not used for primary entrance will be secured from the inside at all times and devoid of external locking hardware. The doors will be equipped with appropriate hardware to permit rapid exit from the room or laboratory in the event of fire or other emergency.*
8. The assessor must verify whether procedures for Entry Door Locks have been established and are adhered to.
- ◆ *The following are recommended for Entry Door Locks:*
    - *Exterior doors of buildings containing restricted rooms or laboratories will be secured with only approved locks and locking devices including hasps and chains for each door, depending on the area designation, (e.g., controlled, limited, etc.). U.S. Government key-operated, pin-locking deadbolts that project at least one inch into the door frame or tumbler-type padlocks will be used.*
    - *The main entrance door at an entry control point to a section of a restricted area in a biological facility will be secured by a minimum of two key-operated deadbolt locks. Individual laboratory rooms, located within the controlled area, will be secured with a minimum of one lock on each main entrance door or an approved electronic locking system. The lock will be a key-operated deadbolt with a one inch throw or a medium security padlock. All biological select agent and toxins containers will be secured with manufacturer-installed locking hardware or retrofitted with a manufacturer-approved electronic lock integrated into the facility's electronic security system. Other doors not ordinarily used for access will be secured on the interior and will provide resistance to penetration equivalent to that of the structure itself. Doors will be secured by a substantial locking bar or dead bolt from inside the structure or by low security padlocks with steel hasps.*
    - *Specifications for other types of locks will accord with those listed in AR 190-XX.*
9. The assessor must verify whether illumination is sufficiently addressed and that security lighting is provided for entrance doors to rooms or laboratories that qualify as restricted areas.
10. The assessor must verify whether sufficient procedures for Restricted Areas have been established and are adhered to.
- ◆ *The following are recommended for restricted areas.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- *Biosafety Level (BSL) 3 and 4 facilities and laboratories containing select agents will be designated as restricted areas by a responsible official. Biological select agents and toxins will be secured in an exclusion area within a limited area. The restricted areas will be designated according to the following criteria:*
    - *The limited area will be designated as the inside of a room or laboratory or the inside of a suite of laboratories, containing select agents or sensitive materials.*
    - *The controlled area will be designated outside or surrounding a limited area. Entry to the controlled area is restricted to personnel with a need for access. The controlled area is provided for administrative control, safety or as a buffer zone for in-depth security for the limited or exclusion area.*
    - *The exclusion area will be designated as the inside of a select agent container or individual laboratory rooms that are secured.*
    - *A temporary exclusion area will be designated when the select agent is removed from the secure container. The temporary exclusion area will be the area immediately surrounding the select agent. In the absence of positive measures to prevent physical access by unauthorized persons, access to the temporary exclusion area will constitute access to the select agent.*
    - *Restricted areas and their level of restriction will be designated by appropriate signage, beginning on the outer perimeter fence surrounding the facility.*
11. The assessor must verify whether sufficient procedures for Access Authorization have been established and adhered to.
- ◆ *The following are recommended procedures for access authorization:*
    - *General access to restricted facilities will be limited to authorized personnel with established need. Access will be kept to a minimum and entry control and identification procedures will be established to ensure need for access.*
    - *A roster of personnel authorized to receive keys to laboratories, rooms or containers in restricted areas will be kept current by responsible organizations. The roster will be protected from public view. The roster will be signed by the designated official and contain the names of those individuals authorized to receive keys. Electronic security systems records may be used in lieu of a key control roster for electronic keys, if they are programmed to record and report personnel who have been authorized electronic keys to restricted rooms and laboratories.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- *Access control procedures will be determined and handled by a specified access control officer. This individual will have a clearance at least as high as the material in the restricted areas under his or her control and will be qualified under the applicable personnel reliability programs. The duties of the access control officer will include specifying the location and category of all access-controlled doors, determining the status of all access credentials currently issued, identifying areas of higher security requiring secondary credentials, recommending areas for possible enclave security, recommending credential reissue and recoding schedules and ensuring that access control procedures are known throughout the command through educational programs.*
12. The assessor must verify whether sufficient procedures for Entry Control have been established and adhered to.
- ◆ *The following are recommended procedures for entry control:*
    - *At the entry point to each restricted area, an approved entry control roster (ECR) will be maintained that lists all personnel authorized to enter the restricted area. ECRs will contain the name, Social Security Number (SSN) and organization of such personnel. The responsible official will sign the ECRs.*
    - *Visitors authorized to enter restricted rooms and laboratories will be escorted by personnel who are listed on the ECR and assigned to the facility concerned.*
    - *Records will be kept of approved individuals entering and exiting restricted areas, including date and time of entrance and exit.*
    - *A means of rapid communications and an electronic duress system will be provided to personnel controlling entry into restricted areas to immediately contact additional security personnel for assistance in case of emergencies. Entry control systems will also include rapid entry procedures for emergencies.*
13. The assessor must verify whether sufficient procedures for After Hours Security have been established and adhered to.
- ◆ *The following are recommended procedures for after hours security:*
    - *A responsible authority will establish a system of security checks at the close of each working day to ensure that rooms and laboratories containing select agents or sensitive materials are properly secured. Electronic security systems may be used for this purpose. Responsible personnel will be designated in writing to conduct checks of all select agent containers and doors to restricted rooms and laboratories to ensure they are secured. Actions will be taken to have the intrusion detection systems activated upon exiting and securing the restricted rooms or laboratories.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- *Except in an emergency covered by the facility physical security plan, before a room or laboratory containing restricted agents is opened after normal working hours, authorization will be obtained from the responsible authority. When such an opening is authorized, the facts will be documented. Procedures will be established in the facility security plan to provide for responsible facility personnel to challenge the validity of the authorization, when dictated by the facts and circumstances of the case.*
  - *In recognition that some laboratories and some protocols require around-the-clock access, the responsible authority or designated representative, will provide security personnel with a standing list of after-hours authorizations. Such a list will identify names of researchers authorized and identify the specific laboratories to which they may have access.*
14. The assessor must verify whether sufficient procedures for Package Control have been established and adhered to.
- ◆ *It is recommended that responsible authorities establish a system to control movement of packages and materials into and out of restricted areas. Procedures will be established for inspecting for prohibited items and contraband.*
15. The assessor must verify whether sufficient procedures for Construction/Maintenance Disruption have been established and adhered to.
- ◆ *It is recommended that when substantial construction or maintenance is underway inside restricted areas, the involved portion of the restricted area be physically separated from the areas containing select agents or sensitive materials. This should be accomplished by barriers to impede and delineate entry to the zone of protection associated with the area associated with the critical asset. Added security measures should be taken to detect and prevent entry into the area containing restricted items.*
16. The assessor must verify whether sufficient procedures for Key/Combination Control have been established and adhered to.
- ◆ *The following are recommended procedures for key/combination control:*
    - *Keys or combinations to locks installed on all storage structures for sensitive materials, hazardous materials, buildings, rooms and containers including limited and exclusion areas, IDS access points or perimeter access points, will be strictly controlled and accounted for at all times. These keys/combinations will be maintained separately from other keys/combinations in the facility and accessible only to those individuals whose duties require access to them. Keys/combinations will not be left unattended or unsecured at any time.*
    - *Access to or possession of both keys by only one person to laboratories for which the two-person rule is strictly prohibited.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- *Records will show the disposition of each key to locks on all select agent storage structures, buildings, rooms and containers including limited and exclusion areas. Keys will be held only by those personnel who have been specifically authorized for possession. Records will indicate the names of all personnel who have received combinations to locks for storage areas containing sensitive materials.*
  - *The security and disposition of all keys, combinations and access codes will be the ultimate responsibility of one designated key control official. This official will hold the same level of clearance as those authorized direct access to restricted areas and will also be involved in all applicable personnel reliability programs.*
17. The assessor must verify whether sufficient procedures for Intrusion Detection Systems have been established and are adhered to.
- ◆ *The following are recommended procedures for intrusion detection systems:*
    - *Rooms or laboratories that store select agents will have an approved IDS to detect unauthorized entry, and monitored by security personnel. The use of commercial-off-the-shelf (COTS) IDS is authorized. Maintenance and testing for these off-the-shelf systems will be conducted in accordance with manufacturers requirements. IDS sensors will also be installed on exterior doors and windows of buildings housing High Priority Agents and Toxins (HPA) laboratories/rooms. IDS sensors will be installed inside all restricted laboratories/rooms, to include any openings.*
    - *IDS control units will be placed inside the restricted rooms or laboratories within critical asset facilities or where critical asset materials are maintained. For laboratories equipped with an airlock chamber (i.e., two consecutive entry control doors), IDS control units will be located inside the outer door and immediately adjacent to the inner door.*
    - *Rooms or laboratories within critical asset facilities or that contain high-priority restricted materials that are designated as critical assets will be equipped with a volumetric or motion detector sensor system capable of detecting the entry and movement of an intruder within the protected area. The sensor system will be configured to cover all potential approaches to biological secure containers.*
    - *Security force personnel as specified in the critical asset facility physical security plan will monitor IDS at a manned location with the capabilities to initiate an immediate response. IDS will be in the secure mode (i.e., ready to respond to an intrusion) at all times when the room or laboratory containing select agents or sensitive material is unoccupied. Alarm activation will be displayed at the alarm center. Audio and visual indication will show line supervision and access/secure status. Capability will be provided to conduct a remote self-test of the IDS circuit continuity.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- *IDS will be provided with uninterrupted power supply (UPS), independent of the primary power source that will be capable of operating the system for four hours.*
- *Audible and visual indications that primary power has failed or has been restored will also be provided. The UPS will be kept under surveillance or contained in an alarmed cabinet to protect the system from tampering. The UPS will be tested each quarter or more as recommended by the manufacturer.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF BIOLOGICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>SAFETY PROTOCOLS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Safety Protocols are plans to be enacted by the biological facility designated as a critical asset to prevent a critical disruption in activities due to an accidental event or to deal with an accidental or unpredictable event in a manner that impact activities to the least possible extent.</p>
<p><b><u>INTENT:</u></b> To ensure that the biological facility that is designated critical asset or that houses sensitive material designated as a critical asset faces the least possible disruption from accidental or unpredictable events.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Safety Protocols will address the plans to react to accidental or unnatural events, with the intent of ensuring the least possible impact to the critical asset facility schedule, its capabilities or the critical asset material. Plans to regulate laboratory safety will also be assessed. An assessment will also be performed on plans that address unpredictable situations of all possible natures that may have a deleterious effect on facility capabilities or infrastructure.</p>
<p><b><u>CRITERIA:</u></b> The assessment standards below are based on existing Federal regulations listed in <i>42 CFR Part 73 (undated)</i>. This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below. In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether each approved facility has developed a laboratory safety plan considering the guidelines set forth in the CDC/National Institutes of Health (NIH) publication <i>Biosafety in Microbiological and Biomedical Laboratories</i>.<ul style="list-style-type: none"><li>◆ <i>It is recommended that this plan also incorporate the standards in 29 CFR 1910.1450 and/or 29 CFR 1910.1200.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

2. The assessor must verify whether approved critical asset facilities have developed an emergency response plan (ERP) that meets the requirements of the Occupational Safety Health Administration (OSHA) hazardous waste operations and emergency response standard in 29 CFR 1910.120.
- ◆ *It is recommended that the ERP also be coordinated with other facility-wide plans, (i.e., natural disasters, power outages, severe weather or other plausible emergencies). The ERP should also consider the effects of the response on the spread or transfer of select agents (including planning and coordination with outside parties, personnel roles and lines of authority, safe distances and places of refuge, site security control, decontamination and special procedures needed to address the hazards of select agents and toxins).*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF BIOLOGICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>STORAGE DESIGN CRITERIA</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Storage Design Criteria refers to the prescribed storage and biosafety procedures that are followed to ensure the safety, stability and containment of etiologic agents or sensitive material within biological critical asset facilities.</p>
<p><b><u>INTENT:</u></b> To ensure that select biological agents and facilities designated as critical assets are properly safeguarded to preclude facility contamination, accidental release, sabotage, theft, loss, seizure or unauthorized access.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Storage Design Criteria will address the capability of the biological critical asset facility to contain both select agents and sensitive materials relating to them. Laboratory storage apparatus will be considered, as well as their physical and operational security. Physical features contributing to the security of stored information (e.g., facility layout, access control, etc.) will be assessed.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Storage Design Criteria are based on guidelines contained in <i>AR 190-XX: Biological Security (Draft), Biological Security -Biosafety in Microbiological and Biomedical Laboratories, 4<sup>th</sup> ed. (undated)</i>, and the <i>NIH Policy Manual (undated)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this topic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether sufficient Laboratory Storage Criteria has been established and adhered to.<ul style="list-style-type: none"><li>◆ <i>The following are recommended laboratory storage criteria:</i><ul style="list-style-type: none"><li>➤ <i>Critical asset facility design criteria (e.g., primary and secondary barriers, etc.) will be commensurate with the specified biosafety level of the laboratory and the agents it contains, with respect to appropriate sanitary and decontamination facilities, specialized ventilation systems and airflow controls.</i></li></ul></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- *Checklist-style standards for assessing and determining compliance with a stated biosafety level (Level 1-4) are included in Section 3 of Biosafety in Microbiological and Biomedical Laboratories. These checklists include facility design, laboratory equipment and barriers. Also included are standards for animal containment facilities at all biosafety levels.*
  - *There will be proper alignment between the designated biosafety level of stored agents and the biosafety level of the biosafety cabinetry (BSC) in which they are used and/or stored. The facility will be able to demonstrate that proper testing procedures have been completed on Class I and Class II BSC. These will be tested at installation, after a unit has been moved and at least annually thereafter to ensure proper airflow and filtration criteria are met.*
  - *The required criteria to qualify a cabinet to a certain biosafety level will include face airflow velocity, airflow pattern, radionuclide/toxicity allowances and product protection.*
  - *All corridors of buildings will provide for a readily apparent, safe and adequate means that building occupants may exit a building in the event of a fire or other emergency, access and use by emergency personnel, the safe movement of people during normal daily use of the building and the safe transportation of goods and materials.*
2. The assessor must verify whether sufficient Agent Storage Criteria has been established and adhered to.
- ◆ *It is recommended that biological select agents and toxins designated as critical assets or maintained within biological facilities designated as critical assets be stored in any of the following containers, located within appropriately secured exclusion areas:*
    - *Locked laboratory hoods, freezers, laboratory biosafety cabinets, incubators or refrigerators.*
    - *Locally fabricated or purchased containers of at least 20 gauge steel, or material of equivalent strength, (e.g., grillwork, screening, clear structural material such as impact resistant polymer, etc.).*
    - *Built-in containers constructed of at least 20-gauge steel or material of equivalent strength, mounted in concrete at counter top level.*
    - *Security containers, vaults, safes or secured rooms described in AR 380-5 for storage of classified material (i.e., any classification designation).*
3. The assessor must verify whether sufficient Backup Power Generation has been established, maintained and in use.

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- ◆ *It is recommended that in addition to the primary electric power, all sites will have standby generator power. Standby generator power will be adequate to provide electricity for on-site security and communications functions, have an automatic or remote start capability, be able to assume the full essential on-site load within 60 seconds of a primary power interruption and will be tested at least each week under full load to ensure it will be operable when needed.*
4. The assessor must verify whether sufficient Agent Compartmentalization procedures have been established and adhered to.
- ◆ *It is recommended that compartmentalization, when used in conjunction with a two-person rule (i.e., no single individual can have access to an asset without the knowledge or presence of a second person) provides additional security protection for critical information and assets. If all employees within a controlled area do not require access to all assets, the assets should be compartmentalized in separate limited areas within the controlled area.*
5. The assessor must verify whether sufficient procedures for Classified Storage have been established and adhered to.
- ◆ *It is recommended that classified components be stored in compliance with AR 380-5. Responsible officials should prescribe supplementary controls to prevent unauthorized access and ensure the classified components are accounted for at all times. Personnel whose duties require access to the storage structures will have a security clearance commensurate with the classification concerned.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF BIOLOGICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>MATERIAL CONTROL AND HANDLING PROCEDURES</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Material Control and Handling Procedures refers to those processes that maintain the integrity of sensitive materials, etiologic or otherwise, when in use at each biological facility associated with critical assets. This will include the highest standards for laboratory working methods, accountability and transportation security.</p>
<p><b><u>INTENT:</u></b> To ensure that critical asset material maintained in a biological facility is subject to the most professional standards of transportation, accountability and laboratory method.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Material Control and Handling Procedures will ensure that the scientific work performed in the facility is in compliance with all applicable regulations and professional standards. In addition, the prevalence of safety inspections and risk assessment procedures to reduce the risk of accidental infection or facility contamination will be assessed. An assessment will also address the recordkeeping functions associated with laboratory contents, including those mandated by applicable federal law.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of storage design criteria are based on guidelines contained in 42 CFR Part 73 (undated), <i>Biosafety in Microbiological and Biomedical Laboratories, 4<sup>th</sup> ed. (undated)</i>, and the <i>NIH Policy Manual (undated)</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this topic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether sufficient requirements for a designated Material Control and Handling Official have been established and adhered to.<ul style="list-style-type: none"><li>◆ <i>The following are recommended requirements for the designated responsible official:</i><ul style="list-style-type: none"><li>➤ <i>Each authorized facility will have a responsible official for ensuring the standards are met.</i></li></ul></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- *This person will have passed a personal security risk assessment under Part 73, be familiar with the regulations, have the authority to enforce the regulations and develop and implement a safety, security and emergency response plan. The responsible official will allow only authorized personnel access to select agents, provide appropriate training to staff, ensure select agents are transferred appropriately, is responsible for maintaining an inventory of select agents and is responsible for providing timely notice of loss or theft. The responsible official will also maintain detailed records of information necessary to give a complete accounting of all activities related to select agents or toxins designated as critical assets.*
2. The assessor must verify whether sufficient Laboratory Protocols for Select Agents have been established and adhered to.
- ◆ *The following are recommended laboratory protocols for select agents:*
    - *Freezers, cabinets, or containers where select agents are stored are required to be secure (e.g., such as inside lock boxes) when not in direct view of cleared personnel.*
    - *Packages entering or leaving a restricted area will be inspected. Also, policies will exist for intra-facility movement of agents from laboratory to laboratory to ensure accountability and security.*
    - *Individuals authorized to access select agents or sensitive materials will not share their means of access (e.g., pass cards, keys, combinations, etc.) with any other person, regardless of security status.*
3. The assessor must verify whether sufficient Material and Personnel Recordkeeping Requirements have been established and adhered to.
- ◆ *The following are recommended material and personnel recordkeeping requirements:*
    - *Approved facilities will maintain an accurate record of employees to include data submitted for personal risk assessments and the authorization expiration dates for cleared personnel.*
    - *Accurate records and inventories of each select agent and toxin will be maintained onsite. These will name the agent, give the source of the agent and date of acquisition, list the quantity of the agent, record any destruction of samples, describe the date, sender and recipient of an agent if transferred and catalog any lost or unaccountable samples. All uses of select agents and toxins will be recorded including the individual accessing the agent, date, reason for use, amount removed and amount returned. The facility will ensure that all records, inventories, license documents and personnel clearance forms are kept current and accurate.*
4. The assessor must verify whether sufficient procedures for a Laboratory Risk Assessment have been established and adhered to.

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- ◆ *It is recommended that each laboratory group working with BSL 3 or 4 agents will conduct periodic risk assessments. Each laboratory group will review laboratory operations and agent handling protocols to identify potential risks of self-infection or facility contamination. Risk assessments will be completed by the laboratory director or principal investigator. Risk assessment will ensure that agents are handled and stored in facilities of a suitable BSL and that personnel follow proper risk-reducing laboratory techniques.*
5. The assessor must verify whether sufficient procedures and requirements for Corridor Safety have been established and adhered to.
- ◆ *It is recommended that the biological facility have a facility-wide policy for the temporary corridor placement of flammable or combustible liquids, hazardous chemicals, liquefied gasses, radioactive materials and biological agents. No waste containers will be left in corridors, including those for general, medical, pathological, chemical, radioactive or mixed wastes. All materials stored in corridors will be placed within metal cabinetry.*
6. The assessor must verify whether sufficient Toxin Safety Protocols have been established and adhered to.
- ◆ *The following are recommended toxin safety protocols:*
    - *Toxins are also etiologic materials that require strict materials handling requirements. Toxins can be classified as BSL 2 or BSL 3 agents and the appropriate handling methods will be followed for handling. Each relevant laboratory will produce a toxin safety plan that addresses the specific hazard and safety protocols necessary for working with a particular toxin. An inventory control system will be in place as part of the overall select agent inventory process.*
    - *Toxins will be kept in locked containers when not in use, and access will be limited to only those personnel whose work assignments require access. Proper operation of tools and cabinetry will be assured and proper sanitization measures will be maintained for handling and transport of the toxin within the facility.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF BIOLOGICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>SECURITY FORCE OPERATIONS (SFO)</i></p>
<p><b><u>SUBTOPIC:</u></b> N/A</p>
<p><b><u>EXPLANATION:</u></b> Security Force Operations (SFO) refers to designated persons specifically organized, trained and equipped to provide physical security and perform law enforcement tasks in the safeguarding of biological agents designated as critical assets and the protection of their storage sites.</p>
<p><b><u>INTENT:</u></b> To ensure that the principles, plans, tactics, procedures and equipment used by the Security Force are sound and capable of repelling an adversary force.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of SFO will include the physical requirements outlined in the site security plan and in applicable regulations. The programs and efforts that go into the development, evaluation and revision of the site security plan will address the specific and anticipated localized threat including threat detection, delay, identification, assessment, response, recovery and other measures necessary to protect the designated biological critical assets. The provisions of these standards will be applicable to all biological agent storage sites.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of SFO are based on the <i>Army Regulation 190-XX: Biological Security (Draft)</i>. This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below. In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether there are sufficient security forces assigned and designated in the site security plan to satisfy the necessary security requirements for the site.<ul style="list-style-type: none"><li>◆ <i>It is recommended that security forces are organized, trained, manned and equipped to provide normal day-to-day protection for chemical agents and to react to security incidents involving chemical agents.</i></li></ul></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

2. The assessor must verify whether responsible officials ensure that only qualified personnel are used to safeguard biological agents/facilities, and take necessary actions to ensure that security force personnel who do not meet PRP requirements are not assigned to protect biological storage sites.
  - ◆ *It is recommended that the standards in AR 190-56 will be applicable to civilian security guards assigned to biological agent/facility security duties.*
3. The assessor must verify whether security force sentries on post are forbidden to use recreational materials while performing their duties.
4. The assessor must verify whether security force personnel are only tasked to perform security functions while on duty.
  - ◆ *It is recommended that responsible officials monitor and evaluate overtime hours and take appropriate action to preclude excessive overtime by security force guards.*
5. The assessor must verify whether written orders/directions covering site security will be provided for each guard post and security force patrol.
  - ◆ *It is recommended that orders will either be carried by the security forces or be available for use at the site. The orders will include instructions on the use of force.*
6. The assessor must verify whether responsible officials ensure there are sufficiently trained security force guards to control entry and to prevent unauthorized access to critical asset facilities/site containing biological agents.
  - ◆ *It is recommended the security forces consist of a Backup Force (BF), Reaction Force (RF) and Alert Force (AF).*
  - ◆ *It is recommended that a portion of the site RF will be deployed in a random manner in either fixed observation or fighting positions and as mobile foot or vehicle patrols. Posted security force sentries will not be a part of the RF numerical requirement and will continue their assigned tasks when the RF is deployed.*
7. The assessor must verify whether the RF conducts training exercises to maintain proficiency.
8. The assessor must verify whether the security force is equipped and armed for combat type operations.
  - ◆ *It is recommended that the vulnerability assessment and local surrounding environment be considered in determining the types of weapons to be employed at a biological agent storage site.*
9. The assessor must verify whether tactical defense planning is included in the biological agent site defense plan.
  - ◆ *It is recommended that preplanned weapons fire is set up for the final defense of any storage facilities.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

10. The assessor must verify whether security patrols conduct searches in all areas of possible concealment around the site for indications of the use of such areas for observations and surveillance of site operations by unauthorized personnel.
11. The assessor must verify whether security logs are maintained by the security force to record the chronology of events during a shift.
12. The assessor must verify whether Security forces will have the ability to control entry and to prevent unauthorized access to sites containing biological agents.
  - ◆ *It is recommended that BF capable of responding to attempted penetrations and preventing unauthorized removal of biological agents will be in place at all biological agent storage sites 24 hours a day.*
13. The assessor must verify whether security force members are provided realistic site defense training exercises.
  - ◆ *It is recommended that the training be tailored to each storage site based on the threat and the vulnerability assessment (VA) conducted at the site.*
14. The assessor must verify whether site security forces have developed plans for the recovery of biological agents in the event of their loss.
15. The assessor must verify whether security force plans include inter-organizational support agreements with other service forces to enhance the site security and/or recovery of biological agents.
  - ◆ *It is recommended that inter-service support agreements are used to ensure continuity of support. Plans should be coordinated with organizations providing security forces support to the storage site or activity, to include federal and local civil law enforcement authorities, as applicable.*

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SECURITY OF BIOLOGICAL CRITICAL ASSETS</i></p>
<p><b><u>TOPIC:</u></b> <i>TRAINING</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>N/A</i></p>
<p><b><u>EXPLANATION:</u></b> Biological Security Training refers to the training and exercise program designed to assure the attainment and maintenance of the critical asset staff's and security forces' capability to protect biological agents from unauthorized access, damage or sabotage, unauthorized destruction, loss of custody, capture or theft and unauthorized use during all phases of its life cycle.</p>
<p><b><u>INTENT:</u></b> To ensure that the critical asset staff and security force personnel involved in the protection of biological critical assets receive the basic and specialized training necessary to attain the skills they need to apply the security techniques required. Critical asset staff and security force personnel will be trained so that they are capable of early detection and apprehension of intruders, preferably before the intruders have completely penetrated the area perimeter.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Biological Security Training program for critical asset personnel and security forces will include general security training, transportation security training and security supervisory personnel training. The assessment will also include any specialized training pertaining to specific duties assigned and duty location, training exercises and a review of training records maintained for each individual.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Training are based on guidelines contained in <i>AR 190-XX: Biological Security (Draft)</i>. This reference addresses the required areas for assessment of this topic. The baseline reference is supplemented as required and as indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify whether responsible officials have established a basic security-training program to support the specific security needs of the biological critical asset.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Biological Security Standards**

- ◆ *It is recommended that the security program include general training, security skills training, transportation security and security supervisory personnel training.*
- 2. The assessor must verify whether security force personnel have received specialized training, certified by a supervisor, pertaining to their specific duties and duty location.
- 3. The assessor must verify whether responsible officials have established a continuing training/education program to ensure all security force personnel and critical asset staff are able to perform routine duties competently and to meet emergencies quickly and efficiency.
- 4. The assessor must verify whether training records are sufficiently maintained on each individual assigned to the critical asset site.
- 5. The assessor must verify whether force-on-force training exercises are being conducted to improve and maintain the proficiency of site security forces.
- 6. The assessor must verify whether security force personnel have received training so they will be thoroughly knowledgeable of the weapons with which they are armed, to include the proper care, maintenance, safety features, malfunctions and corrective actions and cross-trained and familiar with all weapons available to the security force.
- 7. The assessor must verify whether designated authorities have prescribed the frequency of training in live fire of weapons to ensure acceptable levels of weapon proficiency are developed for security forces armed with such weapons.
  - ◆ *It is recommended that this training meet the requirements in DA Pam 350-38 and AR 190-56 will be used as guidance.*
- 8. The assessor must verify whether responsible officials have determined the adequacy of the security training program through periodic evaluation of the critical asset staff and security force proficiency during response exercises conducted under a variety of different conditions.
- 9. The assessor must verify whether Fire/Emergency Medical Services (EMS) and Hazardous Material (HAZMAT) training complies with applicable requirements of 29 CFR 1910.120, National Fire Protection Association Consensus Standards (NFPA) 472 and 473 and the local, State, Federal or host-nation regulations governing emergency medical services care.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

**SUPPORTING INFRASTRUCTURE**

**DESCRIPTION:**

Supporting infrastructure networks include a consideration of the potential vulnerabilities inherent in the infrastructure “grids” upon which the critical asset resides and from which the asset is supported. Key infrastructure grids include power sources (i.e., natural gas; petroleum, oil, and lubricants (POL); and electric); transportation networks (i.e., railroad, highways, air and seaports); communications (i.e., electronic voice and data communications); and water (i.e., potable and waste).

<b><u>AREA OF CONCERN:</u></b> <i>SUPPORTING INFRASTRUCTURE NETWORKS</i>
<b><u>TOPIC:</u></b> <i>ENERGY</i>
<b><u>SUBTOPIC:</u></b> <i>NATURAL GAS</i>
<b><u>EXPLANATION:</u></b> A natural gas network is comprised of production wells, gathering lines, treatment plants, an extensive piping network, compressor stations, large scale storage tanks and local distribution companies (LDC). The natural gas system is an interconnected network of gathering lines that carry gas from nearby production wells to a pipeline connection or treatment plant. A natural gas system consists of production fields, processing centers, gathering pipelines, transmission pipelines, distribution pipelines, compressor stations, interconnection points, city gates and storage facilities.
<b><u>INTENT:</u></b> To ensure that critical assets are protected from the disruption of natural gas.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of supporting infrastructure natural gas will include an examination of daily consumption, contingency planning, natural gas distribution operation and maintenance, dependence on commercial infrastructure, gas feeds, delivery pressure, review of system drawings, system redundancy, alternate fuels capabilities, pipeline components, system back-up capabilities, peak and annual flow rates, Supervisor Control and Data Acquisition (SCADA) systems, distribution networks and transmission.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

**CRITERIA:**

Standards for the assessment of natural gas infrastructure are based on guidelines contained in *FERC Regulations (undated)*, *U.S. Department of Transportation (DOT) Guidance Manual for Operators of Small Natural Gas Systems, Title 33 – Navigation and Navigable Waters - Waterfront Facilities Handling Liquefied Natural Gas and Liquefied Hazardous Gas, Title 49 – Transportation - Transportation of Natural Gas and Other Gas by Pipeline: Minimum Federal Safety Standard, Federal Safety Standards for Liquefied Natural Gas (LNG) Facilities (49 CFR 193)*, *DoD 4140.25M- DoD Management of Bulk Petroleum Products, Natural Gas and Coal*, and *Defense Program Office for Mission Assurance (DPO-MA) Vulnerability Assessment Guidelines*. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether the site/facility is adhering to all applicable national, federal, state, local, service and specific installation requirements.
2. The assessor must verify whether the site maintains sufficient pre-positioned natural gas and/or alternative fuels inventories to support mission requirements through the period of a likely supply disruption.
3. The assessor must verify whether a current written contingency plan has been developed and coordinated with external gas providers for natural gas systems and associated outages.
  - ◆ *It is recommended that this plan be coordinated with external gas providers and be current.*
  - ◆ *It is recommended that there be adequately trained staff to implement the plan and all operators will be licensed and available to respond onsite at all times.*
4. The assessor must verify whether current drawings, blueprints, maps, schematics and photographs of the natural gas system are available.
  - ◆ *It is recommended that these items be updated annually to reflect current conditions. This information should not be made available to the public, be kept in a secure location and backed-up off site.*
  - ◆ *It is recommended that drawings/maps be maintained in a Geographical Information System (GIS) database and include facility location, size, terrain, location and arrangement of all tanks, pipelines serving the site, drainage systems, pump stations, SCADA systems, pre-positioned natural gas inventories, right-of-ways, emergency shut down systems, spill containment equipment, control stations and interconnections to other systems.*

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

5. The assessor must verify whether the installation/facility performs routine maintenance and testing of on-base natural gas system components to ensure they are in a reliable and safe condition to meet the assigned military mission.
6. The assessor must verify whether the facility/installation performs preventive maintenance to ensure that fuel facility operations are not interrupted due to unplanned equipment failures.
7. The assessor must verify whether the natural gas system has the ability to operate independently of SCADA systems if the SCADA system is not operational.
8. The assessor must verify whether the natural gas system has system back-up capabilities to ensure alternate gas sources, as well as on-site back up generation for continued operation.
9. The assessor must verify whether back-up capabilities (e.g., propane-air, alternate fuels, etc.) are available during peak demand, outages or disruptions in support of mission requirements.
10. The assessor must verify whether natural gas control systems will be properly adjusted to operate within design limits.
11. The assessor must verify whether the natural gas system integrity and reliability are not adversely affected by external, internal or atmospheric corrosion.
12. The assessor must verify whether physical security procedures to include protective enclosure, monitoring and lighting are followed for storage tanks, impounding systems, vapor barriers, cargo transfer systems, process/liquification/vaporization equipment, control rooms, control stations and fire control equipment.
13. The assessor must verify whether the supporting infrastructure adheres to all applicable national, Federal, State, local, service and specific installation requirements.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b> <i>ENERGY</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>PETROLEUM, OIL, AND LUBRICANTS (POL)</i></p>
<p><b><u>EXPLANATION:</u></b> POL is broad term that includes all petroleum and associated products used by the Armed Forces which include all petroleum based and synthetically manufactured materials utilized to fuel, lubricate, preserve, and maintain machinery, equipment, and systems. The POL infrastructure network refers to the POL operations that provide the capability to deploy our Armed Forces anywhere by using the pipeline, containerized, and bulk petroleum for the installation or by moving the materials to sustain DoD operations. These materials include commercial products, Petroleum War Reserve Stocks (PWRS), and Peacetime Operating Stocks (POS). The network also includes all conveyances to deploy and distribute the materials.</p>
<p><b><u>INTENT:</u></b> To ensure that mission critical assets are protected from disruption of POL manufacturing, distribution, and storage systems. For sites/ facilities, to ensure a continuous survivable POL supply to support critical missions.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the POL infrastructure will verify that the system meets required specifications to ensure its capability to meet POL mission support requirements under all contingencies. The assessment will include an examination of system operations and sources, system conditions, distribution, storage and shipment processes. It will include spill prevention and mitigation specifications, monitor and control processes, safety, fire fighting, physical security, contingency planning, conservation and rationing, back up capabilities, and the operation and maintenance of systems to support critical missions.</p>

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

**CRITERIA:**

Standards for the assessment of POL are based on guidelines contained in *Oil Pollution Act (OPA) of 1990, Environmental Protection Agency (EPA) Regulations, North Atlantic Treaty Organization (NATO) Standardization Agreement on Maintenance of Fixed Aviation Fuel Receipt, Storage and Dispensing Systems, Federal Code of Regulations (CFR) - under Title 18 Conservation of Power and Water Resources, Naval Facilities Engineering Command (NAVFAC) MO-230 - Maintenance Manual Petroleum Fuel Facilities, Naval Facilities Engineering Command (NAVFAC) MO-307 - Corrosion Control, Military Handbook 200 (MIL HDBK-200) - Quality Surveillance Handbook for Fuel, Lubricants and Related Products, Joint Publications 4-03 Joint Petroleum and Water Doctrine, Military Handbook 200 (MIL HDBK-200) - Quality Surveillance Handbook for Fuel, Lubricants and Related Products, Military Standard 457 (MIL-STD-457) - Frequency for Inspection and Cleaning of Petroleum Fuel Operating and Storage Tanks, Military Standard 201 (MIL-STD-201) - Military Standardization Handbook Petroleum Operations, Title 33 - Oil Pollution Regulations for Marine Transfer Facilities (33 CFR 154), Title 33 - Oil of Hazardous Material Pollution Prevention Regulations for Vessels (33 CFR 155), Title 33 - Oil and Hazardous Material Transfer Operations (33 CFR 156), DoD 4140.25M - DoD Management of Bulk Petroleum Products, Natural Gas and Coal, American Society for Testing and Materials (ASTM) Standards, and Defense Program Office for Mission Assurance (DPO-MA) Vulnerability Assessment Guidelines. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.*

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether a written contingency plan has been developed for POL systems and associated outages.
  - ◆ *It is recommended that this plan be coordinated with external petroleum and oil providers and should be current. There should be adequately trained staff to implement the plan. All operators should be licensed or otherwise qualified and available to respond on site at all times to support defined critical missions.*
2. The assessor must verify that a comprehensive Fuel Facility Operations Manual that conforms to 33 CFR 154 and state regulations has been prepared and maintained by each Fuel Terminal and Air Station Facility to ensure that all fuel-related operations are conducted in a safe and efficient manner.
3. The assessor must verify that drawings, blueprints, maps, schematics and photographs of the POL system are maintained.
  - ◆ *It is recommended that these items will be updated annually to reflect current conditions. This information should not be made available to the public, be kept in a secure location and be backed up off site.*
  - ◆ *It is recommended that drawings/maps will be maintained in a GIS database and*

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

*include facility location, size, terrain, location and arrangement of all tanks, pipelines serving the site, loading racks, piers, drainage systems, pump stations, SCADA systems, pre-positioned petroleum inventories, right-of-ways, emergency shut down systems, spill containment equipment, control stations and interconnections to other systems.*

4. The assessor must verify whether the installation/facility performs routine maintenance of on-base fuel system components to ensure they are in a reliable condition to meet the assigned military missions.
  - ◆ *It is recommended that the site work with commercial suppliers to ensure that POL facilities operations are not interrupted due to unplanned equipment or delivery failures.*
5. The assessor must verify whether physical security measures, procedures and plans are being followed to support the execution of critical missions.
6. The assessor must verify whether the installation/facility performs proper maintenance of fuel systems to ensure the products' specifications are maintained throughout the on-base distribution system.
7. The assessor must verify whether routine testing of all POL equipment including pumps, valves, loading arms, truck/rail car loading racks, refuelers/defuelers, electric motors, tanks and vessels to ensure procedures for water stripping, line packing, inspection of tanks and compartments, gauging, use of drip and discharge collection from vessels are being followed.
8. The assessor must verify that all POL products have been closely monitored to ensure the quality of the product remains at or above specification.
  - ◆ *It is recommended that the facility samples and tests all fuel products on a strict schedule to ensure they remain within specifications and ensure quality products are delivered in sufficient quantities to support critical mission assets.*
9. The assessor must verify whether the site maintains pre-positioned petroleum inventories in support of wartime requirements and has the capability to accept, store and distribute POL to support critical mission requirements. Bulk and containerized storage capacity must meet all mission requirements.
10. The assessor must verify whether sites/facilities whose missions are dependent on POL, adequately protect and maintain storage, distribution, and processing systems commensurate with the missions they support.
11. The assessor must ensure that sites/facilities whose missions are dependent on POL, ensure effective planning is in place to ensure critical missions are supported to the maximum extent achievable should POL supply be disrupted or degraded.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

12. The assessor must verify whether the site maintains pre-positioned petroleum inventories in support of wartime requirements.
13. The assessor must verify whether bulk storage capacity meets mission requirements.
14. The assessor must verify whether environmental protection procedures address oil spill prevention, waste oil disposal procedures and natural resources management (site specific).
15. The assessor must verify whether the facility will perform preventive maintenance to ensure that fuel facility operations are not interrupted due to unplanned equipment failures.
16. The assessor must verify whether the fuel system has the ability to operate independently of SCADA systems if the SCADA system is not operational.
17. The assessor must verify whether a cathodic protection system is in continuous operation, where applicable, to ensure an effective current and voltage potential is applied to the entire structure.
  - ◆ *It is recommended that routine corrosion surveys be performed to determine the need and most effective method of protection*
18. The assessor must verify whether all mechanical metal parts, components and equipment in a fueling system have been bonded to achieve a balanced static potential throughout the system.
19. The assessor must verify whether a stock system of spare parts is retained on base to guard against possible system shut down for lack of parts.
20. The assessor must verify whether the POL system has system back-up capabilities to ensure alternate POL sources, as well as on-site back up generation for continued operation. The critical asset will adhere and meet all applicable national, Federal, State, local, service and specific installation requirements.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b>  <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b>  <i>ENERGY</i></p>
<p><b><u>SUBTOPIC:</u></b>  <i>ELECTRIC POWER</i></p>
<p><b><u>EXPLANATION:</u></b>          Electric power is produced and transported by a vast electric power transmission network. This network is composed primarily of generating stations, transmission lines, transformers, circuit breakers, switches, control systems (e.g., SCADA), substations and distribution components sites, facilities, assets and systems are dependent on continuous, survivable electrical power to support critical missions. Site/facility power distribution is composed primarily of power distribution components, transformers, switchgear, power generators, back up power systems, uninterruptible power systems, power monitoring and control systems, and power quality devices.</p>
<p><b><u>INTENT:</u></b>          To ensure the distribution network has the capacity, redundancy, path diversity security, survivability, and reliability commensurate with the assets critical missions.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b>          An assessment of Electric Power will include an examination of electric power system capabilities, including peak loads, electrical distribution systems, transmission, back-up generation capabilities, power quality, system redundancy, contingency planning, physical security, commercial infrastructure dependencies, configuration, voltage and capacity. path diversity, power control systems (e.g., SCADA).</p>
<p><b><u>CRITERIA:</u></b>          Standards for the assessment of supporting infrastructure network electric power are based on guidelines contained in <i>North American Electric Reliability Council (NERC) Reliability Standards, Army TM-5683, Navy NAVFAC MO-116, Air Force AF JMAN 32-1083 - Facilities Engineering Electrical Interior Facilities, Army TM5-684, Navy NAVFAC MO-200, Air Force AF JMAN 32-1082 - Facilities Engineering Electrical Exterior Facilities, American National Standards Institute/Institute of Electrical and Electronics Engineers Standard (ANSI/IEEE Std), National Electrical Safety Code (National Fire Protection Association # 70 (NFPA 70)), and Defense Program Office for Mission Assurance (DPO-MA) Vulnerability Assessment Guidelines</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p>

## For Official Use Only

### Draft CIP FSVA Supporting Infrastructure Standards

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether a written contingency plan has been developed for power outages.
  - ◆ *It is recommended that this plan be exercised and updated annually, be appropriately marked, and protected and not be made available to the public.*
  - ◆ *It is recommended that this plan be coordinated with external power providers and should be current.*
  - ◆ *It is recommended that there be adequately trained staff to implement the plan. All operators should be licensed and a sufficient number available to respond to all power emergencies.*
  - ◆ *It is recommended that the site have a Standard Operating Procedure (SOP) for service restoration, load shedding, emergency operations, operation and maintenance.*
  - ◆ *It is recommended that the site/facility remain aware of all national, state, local, DoD, and installation electric power requirements and be in compliance with those standards wherever possible. When requirements do not sufficiently support critical missions or compliance is beyond the control of the site/facility, power continuity and assurance measures should be implemented that assure critical mission accomplishment.*
2. The assessor must verify that Power quality standards are addressed for all sensitive and mission essential equipment. Site/facility power quality and assurance systems should provide clean uninterrupted power to mission critical systems regardless of the quality and availability of commercial power.
3. The assessor must verify whether Drawings, blueprints, maps, schematics, photographs, etc. of the power system have been developed and appropriately maintained and updated.
  - ◆ *It is recommended that should these items be updated annually to reflect current conditions. This information should be appropriately marked and protected, should not be made available to the public, should be kept in a secure location and should be backed up off site.*
  - ◆ *It is recommended that maps and drawings be maintained in Geographic Information System (GIS) and include location of commercial supply, base substation layout, distribution system layout (i.e., above or under ground), switches, backup generation, un-interruptible power supplies and interconnections to other systems.*

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

4. The assessor must verify whether the system has on-site back-up generation (generators) that meet the demand of all critical functions. The reliability, endurance, and redundancy of back-up power systems should support likely worst-case casualty and restoration scenarios based on a thorough threat and vulnerability analysis.
5. The assessor must verify whether the installation/facility has an Electrical Utility Master Plan. This plan should provide for the mitigation and/or elimination of power distribution vulnerabilities associated with critical missions.
6. The assessor must verify whether the electric power system has the ability to operate independently of SCADA systems if the SCADA system is not operational.
  - ◆ *It is recommended that technical personnel qualified to operate and align the electrical distribution system both in the SCADA mode and manual mode must be continuously available.*
  - ◆ *It is recommended that if SCADA is used, the assessment must ensure the SCADA system is secure and not amenable to IT intrusion or attack or system shutdown.*
  - ◆ *It is recommended that SCADA systems have adequate information assurance and security plans policies, procedures, processes, and equipment, to include remote access, if applicable, to ensure mission assurance.*
7. The assessor must verify whether electrical distribution system redundancy, security, and path diversity are commensurate with the criticality of supported missions.
8. The assessor must verify whether the condition of the electric power system has the ability to meet required condition, construction and material standards for the given critical mission. The individual components of the electric power system must have the ability to meet the demands placed on them by critical missions.
9. The assessor must verify whether Power quality standards are addressed for all sensitive and mission essential equipment.
10. The assessor must verify whether the distribution system complies with appropriate design criteria to meet power distribution requirements, including system capacity.
11. The assessor must verify whether the installation has identified the sources of electric power to determine the degree of reliability of the electric power supply and the ability to meet current and future mission requirements.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

12. The assessor must verify whether the electric power commercial network supporting a critical asset meets the requirements for configuration, voltage, and capacity.
13. The assessor must verify whether Electric Power components adhere to physical security recommendations established by the utility or local jurisdiction.
  - ◆ *It is recommended that Point-of-delivery substations that serve the site be secured.*
14. The assessor must verify whether system transmission line status, real and reactive power flow, voltage, Load Tap Change (LTC) settings, frequency and status of reactive resources are sufficiently monitored.
15. The assessor must verify whether all control areas operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.
16. The assessor must verify whether Single point vulnerabilities to critical missions resulting from the collocation of vital electrical systems, lack of redundancy, and/or lack of path diversity are clearly understood.
  - ◆ *It is recommended that measures and planning to mitigate or eliminate these vulnerabilities to include physical and information protection, contingency plans, procedures, installation of new independent systems, and physically separating vital components should be in place.*
17. The assessor must verify whether preventive and corrective maintenance programs are in place.
  - ◆ *It is recommended that these programs be sufficiently staffed by qualified personnel and sufficiently funded to ensure systems provide the reliability commensurate with the missions they support.*
  - ◆ *It is recommended that sufficient spare parts and consumables should be available within the endurance limitations of back-up systems to correct casualties to primary electrical systems supporting critical missions.*
18. The assessor must verify whether the site/ facility primary and back up distribution systems are sufficiently and periodically tested and exercised on an end-to-end basis.
19. The assessor must verify whether disaster preparedness planning, restoration planning, and continuity of operations planning considers and accounts for the robustness of electrical distribution systems and the missions it supports.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

20. The assessor must verify whether operations security is incorporated into all elements of the electrical power processes and operations to include identification of essential elements of friendly information or critical information list, implementation of appropriate measures to protect critical information, and personnel training.
21. The assessor must verify whether Electric Power components sufficiently adhere to physical security recommendations established by the utility or local jurisdiction as a minimum.
- ◆ *It is recommended that point-of-delivery substations that serve the site will be secured.*
  - ◆ *It is recommended that where existing utility, local, and DoD physical security measures do not adequately protect power distribution systems commensurate with a the critical missions it supports, enhanced physical security measures and/or redundant power systems and contingency plans that adequately protect and assure power must be present.*

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b> <i>TRANSPORTATION NETWORKS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>RAILROAD</i></p>
<p><b><u>EXPLANATION:</u></b> Transportation infrastructure network (Rail) refers to the Rail Transportation operations that provide the capability to deploy our armed forces anywhere in the world and the rail logistic effort to sustain them in a conflict. Critical networks include DoD and commercial rail between commercial nodes, between commercial and DoD nodes, between DoD nodes, and within DoD facilities.</p>
<p><b><u>INTENT:</u></b> To ensure the rail networks, nodes, and systems supporting critical missions are protected from disruption, are survivable and nodes have the capacity, security, redundancy, mode and route diversity, and reliability commensurate with the critical missions they support.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the rail infrastructure will include an examination of mission critical rail operations, systems, and assets within DoD installations, between DoD installations, between DoD installations and commercial nodes, and between commercial nodes. Operational areas to be addressed are Command and Control (C2) of rail operations, civil/commercial interdependencies, preparation, and marshalling of cargo for shipment, cargo reception, unit deployment, cargo/ammo loading operations, and port support. The assessment will address railroad systems/assets that are commercially leased, government and commercial owned, the security of the system/asset and the training of the personnel operating/managing the system/asset.. The rail network supporting critical missions will be assessed as a system and bounded with respect to the mission, vulnerabilities to the network, and hazards to the network. Choke points, critical nodes, supporting information and telecommunications systems and networks and other factors that result in rail single point vulnerabilities will be examined to ensure the impacts of the vulnerabilities are understood and mitigated for the range of mission support requirements.</p>

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

**CRITERIA:**

Standards for the assessment of Railroad Transportation systems/assets are based on guidelines contained in the *USTRANSCOM Vulnerability Assessment Elements, Joint Pub 4-01 - Joint Doctrine for the Defense Transportation System, Joint Pub 4-01.3 - Joint Tactics, Techniques, and Procedures for Movement Control, Joint Pub 4-01.5 - Joint Tactics, Techniques, and Procedures for Transportation Terminal Operations, Joint Pub 4-01.7 - Joint Tactics, Techniques, and Procedures for Use of Intermodal Containers in Joint Operations, Joint Pub 4-01.8 Joint Tactics, Techniques, and Procedures for Joint Reception, Staging, Onward Movement, and Integration, Joint Pub 4-01.2 Joint Tactics, Techniques, and Procedures for Patient Movement in Joint Operations, DTR DOD Regulation 4500.9-R-Part I - Passenger Movement, DTR DOD Regulation 4500.9-R-Part II - Cargo Movement, DTR DOD Regulation 4500.9-R-Part III - Mobility, DTR DOD Regulation 4500.9-R-Part IV - Personal Property, DTR DOD Regulation 4500.9-R-Part V - DOD Customs and Border Clearance Policies and Procedures, DTR DOD Regulation 4500.9-R-Part VI - Management and Control of Intermodal Containers and System 463-L Equipment, DOT and FAA Regulations and Standards, applicable International and Host Nation Agreements, all other applicable Service Standards, and Defense Program Office for Mission Assurance (DPO-MA) Vulnerability Assessment Guidelines. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.*

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. In the context of Depot and Installation Operations, the assessor must verify the following:
  - a. The assessor must verify whether C2 activities, elements, and associated physical and cyber assets are protected, survivable, and adequate to support specific mission requirements.
  - b. The assessor must verify whether civil/commercial interdependency activities, elements and assets are protected, redundant, path diverse, and adequate to support specific mission requirements.
  - c. The assessor must verify whether activities, elements and assets are protected and adequate to support specific mission requirements.
  - d. The assessor must verify whether cargo reception-activities, elements and assets are protected and adequate to support specific mission requirements.
  - e. The assessor must verify whether Unit Deployment activities, elements, and assets are protected and adequate to support specific mission requirements.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

- f. The assessor must verify whether cargo/ammo preparation, configuration and loading activities, elements and assets are protected and adequate to support specific mission requirements.
  - g. The assessor must verify whether port support activities, elements and assets are protected, redundant, path diverse and adequate to support specific mission requirements.
2. The assessor must verify whether A written contingency plan and response plan have been developed for loss of railroad transportation assets in the event of primary capability loss.
  - ◆ *It is recommended that this plan be exercised and updated annually and not be made available to the public. There will be adequately trained personnel, and other required resources to activate and execute the plan. The plan should account for the entire range of peacetime, wartime, contingency, and surge missions.*
3. The assessor must verify whether drawings, blueprints, maps, schematics, photographs of railroad transportation assets are available and reflect current conditions.
  - ◆ *It is recommended that this information be exercised and updated annually. This information will not be made available to the public, be kept in a secure location and backed-up off site.*
  - ◆ *It is recommended that drawings and maps be maintained in a GIS database and include the elements, cyber assets and physical assets supporting mission requirements.*
4. The assessor must verify that no single point of failure exists linking any of the operational critical elements, and/or cyber and physical assets, that the impacts of single failure points should be known and planning to mitigate or eliminate the impacts and continue critical missions should be in place, effective, and exercised.
5. The assessor must verify whether Railroad Transportation Operations have on-site back-up generation (generators) and power conditioning (if required for C2, information, communications systems) that will provide adequate power to sustain critical functions.
6. The assessor must verify whether supporting Command, Control, Communications, and Computers (C4) systems are interoperable, flexible, responsive, mobile (if applicable, disciplined, survivable and sustained).

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

7. The assessor must verify whether emergency, security, and repair plans and response assets are commensurate with the criticality of missions and cargoes supported by the rail network, if coordination and planning across assets, functions, and jurisdictions should be in place and if response assets are effective, qualified, trained, and exercised.
8. The assessor must verify whether operations security OPSEC is incorporated into all elements of the rail transportation process and operations to include identification of essential elements of friendly information or critical information list, implementation of appropriate measures to protect critical information, and personnel training.
9. The assessor must verify whether critical mission intra/inter-dependencies have been identified and provided equal attention as the critical railroad transportation assets they support.
10. The assessor must verify whether the installation/site has verified compliance with all DoD, National, Federal, state, local, installation, and any other railroad transportation laws, regulations and/or requirements with regards to the shipment of hazardous material (HAZMAT).

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b>  <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b>  <i>TRANSPORTATION NETWORKS</i></p>
<p><b><u>SUBTOPIC:</u></b>  <i>HIGHWAY</i></p>
<p><b><u>EXPLANATION:</u></b>          Transportation infrastructure network highways refer to any land-based network and/or system that support the movement of ground transportation and supports DoD’s capability to deploy our armed forces.</p>
<p><b><u>INTENT:</u></b>          To ensure that critical assets transported or supported by highway are protected from disruption.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b>          An assessment of highways will include an examination of highway operations, and associated activities, elements, and assets at both the installation and depot level. Operational areas to be addressed are C2 of highway operations civil/commercial interdependencies, preparation, and marshalling of cargo for shipment, cargo reception, unit deployment, cargo/ammo loading operations and port support. The assessment will address highway systems/assets that are commercially leased, government and commercial owned, the security of the system/asset and the training of the personnel operating/managing the system/asset.</p>
<p><b><u>CRITERIA:</u></b>          Standards for the assessment of Highway Transportation systems/assets are based on guidelines contained in <i>United States Transportation Command (USTRANSCOM) and Military Traffic Management Command-Transportation Engineering Agency (MTMC-TEA) Assessment Elements, Joint Pub 4-01 - Joint Doctrine for the Defense Transportation System, Joint Pub 4-01.3 - Joint Tactics, Techniques, and Procedures for Movement Control, Joint Pub 4-01.5 - Joint Tactics, Techniques, and Procedures for Transportation Terminal Operations, Joint Pub 4-01.7 - Joint Tactics, Techniques, and Procedures for Use of Intermodal Containers in Joint Operations, Joint Pub 4-01.8 - Joint Tactics, Techniques, and Procedures for Joint Reception, Staging, Onward Movement, and Integration, Joint Pub 4-01.2 - Joint Tactics, Techniques, and Procedures for Patient Movement in Joint Operations, DTR DOD Regulation 4500.9-R-Part I - Passenger Movement, DTR DOD Regulation 4500.9-R-Part II - Cargo Movement, DTR DOD Regulation 4500.9-R-Part III - Mobility, DTR DOD Regulation 4500.9-R-Part IV - Personal Property, DTR DOD Regulation 4500.9-R-Part V - DOD</i></p>

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

*Customs and Border Clearance Policies and Procedures, DTR DOD Regulation 4500.9-R-Part VI – Management and Control of Intermodal Containers and System 463-L Equipment, Department of Transportation (DOT) and Federal Highway Administration (FHWA) Regulations and Standards, any applicable International and Host Nation Agreements, Defense Program Office for Mission Assurance (DPO-MA) Vulnerability Assessment Guidelines, and all other applicable Service Standards. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.*

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. In the context of Depot and Installation Operations, the assessor must verify the following:
  - a. The assessor must verify whether Command and Control (C2) Operations activities, elements, and associated physical and cyber assets are protected, survivable, and adequate to support specific mission requirements.
  - b. The assessor must verify whether Civil/Commercial Interdependency activities, elements, and assets are protected, survivable, and adequate to support specific mission requirements.
  - c. The assessor must verify whether Cargo Preparation for Shipment and Marshalling activities, elements, and assets are protected, survivable, and adequate to support specific mission requirements.
  - d. The assessor must verify whether Cargo Reception activities, elements, and assets are protected, survivable, and adequate to support specific mission requirements.
  - e. The assessor must verify whether Unit Deployment activities, elements, and assets are protected, survivable, and adequate to support specific mission requirements.
  - f. The assessor must verify whether Cargo/ Ammo Preparation, Configuration, and Loading Operations activities, elements, and assets are protected, survivable and adequate to support specific mission requirements.
  - g. The assessor must verify whether Port Support activities, elements, and assets are protected, survivable, and adequate to support specific mission requirements.
2. The assessor must verify whether A written contingency plan and response plan have been developed for loss of highway Transportation assets in the event of primary capability loss.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

- ◆ *It is recommended that this plan be exercised and updated annually, be appropriately marked and protected, and should not be made available to the public.*
  - ◆ *It is recommended that there are adequately trained personnel, and other required resources to activate, and execute the plan. Additionally, the plan should account for the entire range of peacetime, wartime, contingency, and surge missions.*
3. The assessor must verify whether drawings, blueprints, maps, schematics, photographs of highway transportation assets have been developed and maintained.
- ◆ *It is recommended that these items be appropriately marked and protected and should be updated annually to reflect current conditions. This information should not be made available to the public, should be kept in a secure location and should be backed-up off site.*
  - ◆ *It is recommended that maps be maintained in a Geographical Information Systems database.*
4. The assessor must verify that no single points of failure exist linking any of the operational critical elements, and/or cyber and physical assets, that impacts of single failure points are known and sufficient planning to mitigate or eliminate the impacts and continue critical missions is in place, effective, and exercised.
5. The assessor must verify whether highway transportation operations have on-site back-up generation (generators) and power conditioning (if required for C2, information systems, and communications systems) that provide adequate power to sustain critical functions.
6. The assessor must verify whether critical mission intra/inter-dependencies have been identified, and provided equal attention as the critical highway transportation assets they support.
7. The assessor must verify whether the installation/site has verified compliance with all DoD, National, Federal, state, local, installation, and any other highway transportation laws, regulations, and/or requirements with regards to the shipment of Hazardous Material (HAZMAT).
8. The assessor must verify whether emergency, security, and repair response assets are commensurate with the criticality of missions and cargoes supported by the road network, if coordination across assets, functions, and jurisdictions should be in place and response assets are effective, qualified, trained, and exercised.
9. The assessor must verify whether operations security OPSEC must be incorporated into all elements of the road transportation process and operations to include identification of essential elements of friendly information or critical information list, implementation of appropriate measures to protect critical information, and personnel training.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

- |   |
|---|
| <p>10. The assessor must verify whether supporting C4 systems are interoperable, flexible, responsive, mobile (when applicable), disciplined, survivable and sustained.</p> |
|---|

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b> <i>TRANSPORTATION NETWORKS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>AIR</i></p>
<p><b><u>EXPLANATION:</u></b> Transportation infrastructure network (Air) refers to the airlift operations that provide the capability to deploy our armed forces anywhere in the world and help sustain them in a conflict. Transportation Air critical networks include DoD and civilian networks between commercial nodes, between commercial and DoD nodes, and between DoD nodes.</p>
<p><b><u>INTENT:</u></b> To ensure that mission critical assets transported or supported by air are protected from disruption.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of air transportation will include an examination of refueling, mission preparation and planning, direct air transportation operations, air mobility command and control (C2), total asset visibility/in-transit visibility, processing of passenger and cargo for movement, security, emergency response, load/unload carrier, coordination and monitoring movements between POE, POD, and final destination, coordination of host nation support, coordination of onward movement, monitoring and controlling operations, monitoring day-to-day operations and providing guidance, monitoring deployment data and providing guidance, and staging support. Air operations supporting critical missions will be assessed as a system and bounded with respect to the mission, vulnerabilities, and hazards to operations. Choke points, critical nodes and systems, and other factors that result in air operations single point vulnerabilities will be examined to ensure the impacts of the vulnerabilities are understood and mitigated for the range of mission support requirements.</p>

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

**CRITERIA:**

Standards for the assessment of Air Transportation systems/assets are based on guidelines contained in *Doctrine for the Defense Transportation System (Joint Pub 4-01)*, *United States Transportation Command (USTRANSCOM) and Air Mobility Command (AMC) Assessment Elements Standards, Joint Pub 4-01 - Joint Doctrine for the Defense Transportation System, Joint Pub 4-01.3 - Joint Tactics, Techniques, and Procedures for Movement Control, Joint Pub 4-01.5 - Joint Tactics, Techniques, and Procedures for Transportation Terminal Operations, Joint Pub 4-01.7 - Joint Tactics, Techniques, and Procedures for Use of Intermodal Containers in Joint Operations, Joint Pub 4-01.8 - Joint Tactics, Techniques, and Procedures for Joint Reception, Staging, Onward Movement, and Integration, Joint Pub 4-01.2 Joint Tactics, Techniques, and Procedures for Patient Movement in Joint Operations, Defense Transportation Regulations (DTR) DOD Regulation 4500.9-R-Part I - Passenger Movement, DTR DOD Regulation 4500.9-R-Part II - Cargo Movement, DTR DOD Regulation 4500.9-R-Part III - Mobility, DTR DOD Regulation 4500.9-R-Part IV - Personal Property, DTR DOD Regulation 4500.9-R-Part V - DOD Customs and Border Clearance Policies and Procedures, DTR DOD Regulation 4500.9-R-Part VI - Management and Control of Intermodal Containers and System 463-L Equipment, Department of Transportation (DOT) and Federal Aviation Administration (FAA) Regulations and Standards, International Air Transportation Standards (IATA), USTRANSCOM Vulnerability Assessment Elements, Defense Program Office for Mission Assurance (DPO-MA) Vulnerability Assessment Guidelines, and all other applicable Service Standards. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.*

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. Air Operations:
  - a. The assessor must verify whether Air Transport and Air Refueling Operations activities, elements, and associated physical assets are protected, survivable, and adequate to support specific mission requirements.
  - b. The assessor must verify whether Command and Control (C2) activities, elements, cyber assets, and physical assets are protected, survivable, and adequate to support specific mission requirements.
  - c. The assessor must verify whether Preparing Forces for Movement activities, elements, cyber assets, and physical assets are protected, survivable, and adequate to support specific mission requirements.
  - d. The assessor must verify whether POD & POE Operations activities, elements, cyber assets, and physical assets are protected, survivable, and adequate to support specific mission requirements.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

2. The assessor must verify whether a written contingency plan and response plan has been developed for loss of Air Transportation assets in the event of primary capability loss.
  - ◆ *It is recommended that the plan be exercised and updated annually, be appropriately marked, protected and not be made available to the public. There should be adequately trained personnel, and other required resources to activate, and execute the plan. The plan should account for the entire range of peacetime, wartime, contingency, and surge missions.*
3. The assessor must verify whether drawings, blueprints, maps, schematics, and photographs of Air Transportation assets have been developed and maintained.
  - ◆ *It is recommended that these items should be updated annually to reflect current conditions. This information should be appropriately marked, protected and should not be made available to the public, be kept in a secure location and backed-up off site.*
  - ◆ *It is recommended that maps be maintained in a Geographical Information System (GIS) database.*
4. The assessor must verify that no single points of failure exist linking any of the operational critical elements, and/or cyber and physical assets, that the impacts of single failure points are known and planning to mitigate or eliminate the impacts and continue critical missions are in place, effective, and exercised.
5. The assessor must verify whether air transportation operations have on-site back-up generation (generators) and power conditioning (if required for C2, information systems, and communications systems) that provide adequate power to sustain critical functions.
6. The assessor must verify whether emergency, security, and repair response assets are commensurate with the criticality of missions and cargoes supported by air operations, if coordination across assets, functions, and jurisdictions are in place and response assets are effective, qualified, trained, and exercised.
7. The assessor must verify whether operations security (OPSEC) is incorporated into all elements of the air transportation process and operations to include identification of essential elements of friendly information or critical information list, implementation of appropriate measures to protect critical information, and personnel training.
8. The assessor must verify whether supporting C4 systems are interoperable, flexible, responsive, mobile (when applicable), disciplined, survivable and sustained.
9. The assessor must verify whether critical mission intra/inter-dependencies have been identified, and provide equal attention as the critical air transportation assets they support.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

- |  |
|--|
| <p>10. The assessor must verify whether the installation/site ensures that all DoD, National, Federal, state, local, installation, and any other air transportation laws, regulations, and/or requirements are being met with regards to the shipment of HAZMAT.</p> |
|--|

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<b><u>AREA OF CONCERN:</u></b> <i>SUPPORTING INFRASTRUCTURE NETWORKS</i>
<b><u>TOPIC:</u></b> <i>TRANSPORTATION NETWORKS</i>
<b><u>SUBTOPIC:</u></b> <i>SEAPORTS (SEAPORTS AND PREPOSITIONING)</i>
<b><u>EXPLANATION:</u></b> Transportation infrastructure network (Seaports) refers to the Seaport operations that provide the capability to deploy our armed forces anywhere in the world and help sustain them in a conflict. Subordinate topic seaport includes prepositioning ships.
<b><u>INTENT:</u></b> To ensure that transportation infrastructure systems that support mission critical assets for Sea Port and Pre-Positioning operations are protected from disruption.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of seaports will include an examination of prepositioning operations, and associated activities, elements, and assets. Operational areas to be addressed are sealift allocation, ship operations, C2, left bank, layberth operations, ship reception, ship security, civil/commercial interdependencies, cargo reception, cargo preparation/marshalling, ship loading operations, pre-sailing activities, cargo unloading operations and transportation infrastructure that supports the asset. The assessments will address seaport and prepositioning elements/assets that are commercially leased, government owned, the security of the element/asset and the training of the personnel operating/managing the element/asset.
<b><u>CRITERIA:</u></b> Standards for the assessment of seaports and pre-positioning transportation elements/assets are based on guidelines contained in <i>Joint Pub 4-01 - Joint Doctrine for the Defense Transportation System, Joint Pub 4-01.3 - Joint Tactics, Techniques, and Procedures for Movement Control, Joint Pub 4-01.5 - Joint Tactics, Techniques, and Procedures for Transportation Terminal Operations, Joint Pub 4-01.7 - Joint Tactics, Techniques, and Procedures for Use of Intermodal Containers in Joint Operations, Joint Pub 4-01.8 Joint Tactics, Techniques, and Procedures for Joint Reception, Staging, Onward Movement, and Integration, Joint Pub 4-01.2 Joint Tactics, Techniques, and Procedures for Patient Movement in Joint Operations, DTR DOD Regulation 4500.9-R-Part I - Passenger Movement, DTR DOD Regulation 4500.9-R-Part II - Cargo Movement, DTR DOD Regulation 4500.9-R-Part III - Mobility, DTR DOD Regulation 4500.9-R-Part IV - Personal Property, DTR DOD Regulation 4500.9-R-Part V - DOD Customs and Border Clearance</i>

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

*Policies and Procedures, DTR DOD Regulation 4500.9-R-Part VI – Management and Control of Intermodal Containers and System 463-L Equipment, DOT and the Maritime Administration (MARAD) Regulations and Standards, applicable International and Host Nation Agreements, all other applicable Service Standards, USTRANSCOM Vulnerability Assessment Elements, Defense Program Office for Mission Assurance (DPO-MA) Vulnerability Assessment Guidelines.* The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. In the context of Seaport and Prepositioning Operations, the assessor must verify the following:
  - a. The assessor must verify whether C2 Operations activities, elements and associated physical and cyber assets are adequate to support specific mission requirements.
  - b. The assessor must verify whether Ship Operations activities, elements, and assets are adequate to support specific mission requirements.
  - c. The assessor must verify whether Left Bank activities, elements and assets are adequate to support specific mission requirements.
2. In the context of Seaport Operations, the assessor must verify the following:
  - a. The assessor must verify whether Layberth Operations activities, elements and assets are adequate to support specific mission requirements.
  - b. The assessor must verify whether Ship Reception activities, elements and assets are adequate to support specific mission requirements.
  - c. The assessor must verify whether Ship Security activities, elements and assets are adequate to support specific mission requirements.
  - d. The assessor must verify whether Civil/Commercial Interdependencies activities, elements and assets are adequate to support specific mission requirements.
  - e. The assessor must verify whether Cargo Reception activities, elements and assets are adequate to support specific mission requirements.
  - f. The assessor must verify whether Cargo Preparation/Marshalling activities, elements and assets are adequate to support specific mission requirements.
  - g. The assessor must verify whether Ship Loading Operations activities, elements and assets are adequate to support specific mission requirements.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

3. In the context of Prepositioning Operations, the assessor must verify the following:
  - a. The assessor must verify whether Pre-Sailing activities, elements and assets are adequate to support specific mission requirement.
  - b. The assessor must verify whether Cargo Unloading Operations activities, elements and assets are adequate to support specific mission requirements.
4. The assessor must verify whether the Aids to Navigation (ATON) Systems supporting the port is designed, constructed, and augmented to minimize damage and loss of functionality.
  - ◆ *It is recommended that the ATON system is sufficiently redundant so that failure of one component will not disable the functionality of an aid or the ATON system as a whole.*
5. The assessor must verify whether the terminal has developed protection strategies based upon the structural configuration of piers/wharves in order to limit access to structural areas/members underneath the pier or wharf.
6. The assessor must verify whether the Vessel Traffic Management System (VTMS) supporting the port is designed, constructed, and augmented to minimize damage and loss of connectivity.
  - ◆ *It is recommended that critical nodes (transmitters/receivers, cameras, operations centers, radar/video sites, etc.) should be identified and adequate protection strategies developed to protect them. Back-up utility systems should be designed to meet the requirements for the duration of the expected maximum outage.*
7. The assessor must verify whether utility systems that support critical transportation infrastructure systems are designed, constructed and augmented to minimize damage and loss of functionality.
8. The assessor must verify whether critical mission intra/inter-dependencies between roadway, railway, and waterway transportation system components have been identified, to determine the cascading effects of their loss or neutralization on critical Sea Port and Pre-Positioning operations.
9. The assessor must verify whether a written contingency plan and response plan has been developed for loss of seaport and prepositioning transportation assets in the event of primary capability loss.
  - ◆ *It is recommended that the plan is updated annually and not made available to the public. There should be adequately trained personnel and other required resources to activate and execute the plan.*

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

10. The assessor must verify whether drawings, blueprints, maps, schematics, photographs of seaport and prepositioning transportation assets have been developed and maintained.
  - ◆ *It is recommended that these items be updated annually to reflect current conditions. This information should not be made available to the public, be kept in a secure location and backed-up off site.*
  - ◆ *It is recommended that drawings and maps be maintained in a GIS database and include the elements, cyber assets and physical assets supporting mission requirements.*
11. The assessor must verify that no single points of failure exist linking any of the operational critical elements, and/or cyber and physical assets, that the impacts of single failure points are known and planning to mitigate or eliminate the impacts and continue critical missions are in place, effective, and exercised.
12. The assessor must verify whether seaport and prepositioning transportation operations have on-site back-up generation (generators) that will provide adequate power to sustain critical functions.
13. The assessor must verify whether supporting C4 systems are interoperable, flexible, responsive, mobile (when applicable), disciplined, survivable and sustained.
14. The assessor must verify whether the installation/site complies with all applicable DoD, national, Federal, State, local, installation, and any other seaport and prepositioning operations laws, regulations, and/or requirements with regards to the handling and shipment of HAZMAT.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b> <i>COMMUNICATIONS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>ELECTRONIC VOICE AND DATA COMMUNICATIONS</i></p>
<p><b><u>EXPLANATION:</u></b> Electronic Voice and Data Communications refers to any access, transmission, emission or reception of signs, signals, writings, images, sounds or information of any nature by wire, radio, visual or other electromagnetic system.</p>
<p><b><u>INTENT:</u></b> To ensure that critical assets are protected from disruption of communications systems.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of communications systems will include an examination of Transmission Media which includes antenna's, repeaters, microwave, cable head-end's, optical fiber head-end's, above ground local loop systems, underground local loop systems and customer premise systems, Private Branch Exchange, Local Area Networks and Dial Central Offices; Terminal devices which include, computers, servers, data centers, and communications processors; Switches which include Remote Units, Points of Presence, Access Tandems, Mobile Switching Centers and routers; Control components which include devices such as Network Operations Centers, Defense Enterprise Computing Centers, System Management Centers, Network Operations and Security Centers, Computer Emergency Response Team, Network Enhanced Mobile Satellite Services, Bandwidth Managers, Signaling. The assessment will address communications systems that are commercially leased, government owned, the physical security of the system and the training of personnel operating/managing the system.</p>
<p><b><u>CRITERIA:</u></b> Standards for the assessment of electronic voice and data communications infrastructure are based on guidelines contained in <i>Joint Pub 06 - Command, Control, Communication and Computer Systems Support to Joint Operations</i>, <i>DoD Joint Technical Architecture (JTA)</i>, <i>DISA Circular C-310-1</i>, and <i>Defense Program Office for Mission Assurance (DPO-MA) Essential Elements of Information (EIs)</i> and established best practices for the assessment of critical infrastructure. The applicable portions of the</p>

## For Official Use Only

### Draft CIP FSVA Supporting Infrastructure Standards

above listed references are listed below and collectively address the required areas for assessment of this subtopic. The assessor must verify whether DoD components have ensured that government-owned communications equipment, systems, facilities and networks are effectively and efficiently operated and maintained to meet the demands placed on them.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether a written contingency plan and response plan have been developed for loss of communications and rerouting of communications in the event the main telephone exchange is lost.
  - ◆ *It is recommended that this plan is updated annually and not made available to the public. There should be adequately trained staff to implement the plan. Operators should be available to respond on-site at all times.*
2. The assessor must verify whether drawings, blueprints, maps, schematics, and photographs of the communications system have been developed and maintained.
  - ◆ *It is recommended that these items be updated annually to reflect current conditions. This information should not be made available to the public, be kept in a secure location and backed-up off site.*
  - ◆ *It is recommended that drawings and maps be maintained in a GIS database and include network diagrams, connectivity diagrams, latitudes and longitudes.*
3. The assessor must verify that no single point of failure will exist in paths linking network elements deemed critical to the operations of a network.
  - ◆ *It is recommended that network operators ensure that networks built with redundancy are also built with geographic separation. The site should avoid placing mated pairs in the same location, avoid redundant logical facilities in the same physical path, avoid placing redundant equipment and functions in the same building complex. Diverse network management systems should also be considered.*
4. The assessor must verify whether the system has on-site power generation (e.g., generators) and Heating, Ventilation, and Cooling (HVAC) systems that meet the demands of all critical functions.
5. The assessor must verify whether the critical asset ensures that all applicable National, Federal, state, local installation and military communications requirements are being met.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b> <i>WATER SYSTEMS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>POTABLE, INDUSTRIAL, AND FIRE FIGHTING WATER</i></p>
<p><b><u>EXPLANATION:</u></b> Water systems are the means by which water is extracted, treated, stored and delivered to consumers. Consumers may be people, facilities or functions such as fire fighting or HVAC. In many instances one system supports all functions while, storage tanks, wells, and reservoirs provide redundant or back up capabilities. For sites/facilities, assets are dependent on a continuous, protected, and survivable water supply to support critical missions. Site/facility water systems are composed of supply, distribution, pumping, treatment, filtering, storage, and reserves components.</p>
<p><b><u>INTENT:</u></b> To ensure that water systems support mission critical assets, are available, and protected from disruption. To ensure that water reserves, processes, and planning will support critical missions should water supply be disrupted.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of a water systems infrastructure will verify that the systems meet required specifications to ensure their capability to meet water demand associated with critical missions, force sustainment, and protection. The assessment will include an examination of supported critical missions, system usage and sources, system conditions, water treatment, processing, and filtering, system capacities, monitor and control processes, storage, quality, distribution, physical security, contingency planning, conservation and rationing, back-up capabilities, and operation and maintenance of the system.</p>
<p><b><u>CRITERIA:</u></b> The standard for the assessment of supporting infrastructure network water systems are based on guidelines contained in the Safe Drinking Water Act (SWDA) of 1974, National Primary Drinking Water Regulation (NPDWR), American Water Works Association (AWWA) standards, Title 40 --Protection of the Environment, National Primary Drinking Water Regulations Implementation, State Underground Injection Control Program, Public Health Security and Bioterrorism Preparedness and Response Act of 2002, DoD Instruction 2000.18, DoD 2000.16, and the Defense Program Office for</p>

## For Official Use Only

### Draft CIP FSVA Supporting Infrastructure Standards

Mission Assurance (DPO-MA) Vulnerability Assessment Guidelines. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether the water system adheres to specified potable, fire fighting, and industrial water treatment processes and regulations and meet criteria defined by the missions it supports.
2. The assessor must verify whether water treatment plant components must adhere to physical security recommendation established by the utility or established by the local jurisdiction for the given locale.
3. The assessor must verify whether conveyance and distribution system components adhere to physical security regulations for the given locale and/or commensurate with the critical missions the systems support.
4. The assessor must verify whether a written contingency plan has been developed for water systems and associated outages.
  - ◆ *It is recommended that water conservation and rationing planning should consider missions supported, endurance of on site supplies, and priorities for available supplies.*
  - ◆ *It is recommended that this plan is coordinated with external water providers and should be current. There should be adequately trained staff to implement the plan. All operators should be licensed and available to respond on site at all times.*
  - ◆ *It is recommended that contingency planning is coordinated with other site/facility emergency plans. A water disruption could quickly trigger the evacuation of non-essential personnel as a means to support sustained mission operations.*
5. The assessor must verify whether the water system has system back-up capabilities to ensure alternate water sources, as well as on-site back up generation for treatment plants and booster stations.
  - ◆ *It is recommended that if alternate sources are not available, contingency planning to conserve and ration water to best sustain critical missions should be in place. In addition to potable water, many critical missions depend on the availability of water. Fire fighting, mission critical HVAC systems, aircraft wash down facilities and industrial facilities depend on water supply.*
6. The assessor must verify whether system water capacity will meet the required consumer demand.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

7. The assessor must verify whether the distribution system is divided into to multiple pressure zones to make isolation of areas easier and supply priority demands if required.
8. The assessor must verify whether onsite water storage facilities and back up water sources meet the capacity requirements for water to include potable, fire fighting, and industrial requirements and that storage amounts meet installation guidelines and critical mission support criteria.
9. The assessor must verify whether the site/facility has ensured that all national, state, local, and installation water requirements are being met.
  - ◆ *It is recommended that where critical missions require, these standards shall be exceeded and be commensurate with the missions supported.*
10. The assessor must verify whether sufficient spare parts, equipment, and consumables are readily available to maintain systems, restore disruptions to systems, and provide for the transportation of emergency water supplies to support missions disrupted by a loss of water supply.
11. The assessor must verify whether water supply personnel and systems are periodically tested and exercised under likely scenarios that would deprive water to critical missions.
12. The assessor must verify whether the condition of the water system meets the required condition, age, construction and material standards for the given locale and the individual components of the water system have the ability to meet the demands placed on them.
13. The assessor must verify whether the water system adheres to specified water treatment processes and regulations.
  - ◆ *It is recommended that treatments, chemicals and coatings in contact with drinking water will be certified as meeting industry consensus standards for water contact or treatment. Water samples should be taken in accordance with SDWA regulations. The water system should have a written sampling plan approved by the state.*
14. The assessor must verify whether distribution networks meet demand requirements to ensure effective flow and pressure.
15. The assessor must verify whether treatment plant components adhere to physical security recommendations established by the utility.
  - ◆ *The following are physical security recommendations for treatment plant components:*
    - *Water treatment plant works will be locked and secured.*
    - *Proper lighting, cameras and alarms will be in use.*

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

- *All stored chemicals will be secured.*
  - *Vaults, pits, and back flow prevention devices will be secured.*
16. The assessor must verify whether conveyance and distribution system components adhere to physical security regulations.
- ◆ *The following are physical security recommendations for conveyance and distribution system components:*
    - *Pump stations and wells will be secured.*
    - *Water tanks will be secured.*
    - *Open reservoir will be secured.*
    - *Intake structures will be secured.*
    - *Components will have proper lighting, cameras and alarms.*
    - *Vaults, pits and backflow prevention devices will be secured.*
17. The assessor must verify whether, in areas of low pressure or high risk, backflow prevention devices are used.
18. The assessor must verify whether drawings, blueprints, maps, schematics, and photographs of the water system have been developed and maintained.
- ◆ *It is recommended that these items will be updated annually to reflect current conditions. This information should not be made available to the public, be kept in a secure location and be backed up off site.*
  - ◆ *It is recommended that drawings are maintained in a GIS database and include plant location with detailed treatment process information included in the attribute table, pump locations, pipe size, date of installation, pipe material type, valve and blow off locations, storage tank locations with capacities, hydrant locations and interconnections to other systems.*
19. The assessor must verify whether the water system is operated and maintained in accordance with the local controlling authorities rules and regulations.
20. The assessor must verify whether onsite water storage facilities meet the capacity requirements for potable water and that storage amounts satisfy installation guidelines.
21. The assessor must verify whether the water system has the ability to operate independently of SCADA systems if the SCADA system is not operational.
22. The assessor must verify whether the facility ensures that all applicable National, Federal, State, local and installation water requirements are being met.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b>  <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b>  <i>WATER</i></p>
<p><b><u>SUBTOPIC:</u></b>  <i>WASTEWATER</i></p>
<p><b><u>EXPLANATION:</u></b>  Wastewater refers to sewage, storm water and water that has been used for various purposes around the community. Unless properly treated, wastewater can harm public health and the environment. Most communities generate wastewater from both residential and nonresidential sources.</p>
<p><b><u>INTENT:</u></b>  To ensure that critical assets are protected from disruption of wastewater systems.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b>  An assessment of wastewater systems will include an examination of wastewater treatment and collection processes/systems, system condition, maintenance, operations, back-up capabilities, storage requirements, contingency planning, wastewater rerouting, hazardous materials management and physical security.</p>
<p><b><u>CRITERIA:</u></b>  Standards for the assessment of waste water systems are based on guidelines contained in the <i>Clean Water Act (CWA), Pollution Prevention Act, Safe Drinking Water Act (SDWA), Federal Water Pollution Control Act, National Environmental Policy Act, Guidelines for Storage and Collection of Residential, Commercial and Institutional Solid Wastes, Hazardous Waste Restrictions, Criteria for Classification of Solid Waste Disposal Facilities and Practices, Standards for Owners and Operators of Hazardous Waste Treatment, Storage and Disposal Facilities, and DPO-MA Vulnerability Assessment Guidelines</i>. The applicable portions of the above listed references are listed below and collectively address the required areas for assessment of this subtopic.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"> <li>1. The assessor must verify whether wastewater plant components adhere to physical and information/control system security recommendations established by the utility or established by the local jurisdiction for the given locale. <ul style="list-style-type: none"> <li>◆ <i>The following are physical security recommendations for wastewater plant components:</i></li> </ul> </li> </ol>

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

- *Wastewater treatment plant works will be locked and secured.*
  - *Proper lighting, cameras and alarms will be in use.*
  - *All stored chemicals must be secured.*
  - *Vaults, pits and back flow prevention devices should be secured.*
2. The assessor must verify whether the wastewater system has the ability to operate independently of SCADA systems if the SCADA system is not operational.
- ◆ *It is recommended that if SCADA is used then the assessment must ensure the SCADA system is secure and not amenable to IT intrusion or attack, system shutdown, or catastrophic manipulation of the wastewater system or release of stored chemicals. SCADA systems should have adequate information assurance and security plans policies, procedures, processes, and equipment, to include remote access, if applicable, to ensure mission assurance.*
3. The assessor must verify whether the installation/facility provides local fire and rescue services with information on the types and locations of hazardous materials.
4. The assessor must verify whether the wastewater system has sufficient back-up capabilities.
- ◆ *It is recommended that back-up generators be available and tested monthly under load to verify operation. Generators should be capable of operation (fuel, load capacity, maintenance schedules) in excess of longest historical or expected power outages.*
5. The assessor must verify whether wastewater collection systems within other jurisdictions that connect to the system being assessed have been examined to ensure no vulnerabilities exist, if the impacts to critical missions of single failure points should be known and planning to mitigate or eliminate the impacts and continue critical missions should be in place, effective, and exercised.
6. The assessor must verify whether mission critical facilities such as C2 sites (especially underground sites) that are required to be manned by significant numbers of personnel in continuous and sustained operations and in all threat environments, wastewater systems supporting those assets are redundant, protected, available, and survivable.
7. The assessor must verify whether operations security OPSEC has been incorporated into all elements of the waste water process and operations to include identification of essential elements of friendly information or critical information list, implementation of appropriate measures to protect critical information, and personnel training.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

8. The assessor must verify whether wastewater collection and treatment processes and systems adhere to all local and Federal standards.
9. The assessor must verify whether the condition of the wastewater system meets the required condition, age, construction and material standards for the given area and the individual components of the waste water system have the ability to meet the demands placed on them.
10. The assessor must verify whether onsite chemical storage facilities meet the capacity requirements for wastewater systems and if storage amounts meet installation/facility guidelines.
11. The assessor must verify whether a written contingency plan and response plans for loss of wastewater collection and/or treatment has been developed and maintained.
  - ◆ *It is recommended that this plan be coordinated with external treatment facilities. There will be adequately trained staff to implement the plan. All operators should be licensed and available to respond on-site at all times.*
  - ◆ *It is recommended that the plan be exercised and updated annually, be appropriately marked and protected and should not be made available to the public. The plan should account for the entire range of peacetime, wartime, contingency, and surge missions.*
12. The assessor must verify whether drawings, blueprints, maps, schematics and photographs of the wastewater system have been developed and maintained.
  - ◆ *It is recommended that these items be updated annually to reflect current conditions. This information will not be made available to the public, be appropriately marked and protected, should be kept in a secure location and be backed up off-site.*
  - ◆ *It is recommended that drawings are maintained in a GIS database and include plant location with detailed treatment process information included in the attribute table, pump locations, pipe size, date of installation, pipe material type, storage tank locations with capacities and interconnections to other systems.*
13. The assessor must verify whether the installation maintains wastewater re-routing plans to maintain critical functions.
14. The assessor must verify whether the installation/facility conducts proper management of hazardous materials.
15. The assessor must verify whether chemicals and other hazardous materials are stored and handled in an appropriate manner.
16. The assessor must verify whether the wastewater system is operated and maintained in accordance with the local controlling authorities rules and regulations.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

- |   |
|---|
| <p>17. The assessor must verify whether the site/installation has ensured that all national, Federal, State, local, installation and service wastewater requirements are being met.</p> |
|---|

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>SUPPORTING INFRASTRUCTURE NETWORKS</i></p>
<p><b><u>TOPIC:</u></b> <i>SUPPORTING UTILITIES</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>HEATING, VENTILATION, AND AIR CONDITIONING (HVAC)</i></p>
<p><b><u>EXPLANATION:</u></b> Environmental control via HVAC systems supports a wide variety of critical missions associated with assets and facilities. Environmental control consists of subsystems that include refrigerated cooling, heating, humidity control, waste heat removal, and fresh air ventilation.</p>
<p><b><u>INTENT:</u></b> To ensure critical mission assets are protected from the disruption of vital environmental control. To ensure environmental control systems have the capacity, redundancy, and reliability commensurate with vital missions they support.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> Command and control, computer, communications, intelligence and other mission critical assets are dependent on reliable and survivable environmental systems to sustain asset systems operations and personnel. An assessment of environmental controls will include an examination of HVAC and other systems capabilities that provide reliable and survivable support to ensure the sustained operations of vital mission assets.</p>
<p><b><u>CRITERIA:</u></b> Standards for the assessment of mission critical environmental controls were derived from the following: DoD Unified Facilities Criteria (UFC). Design Refrigeration Systems for Cold Storage. UFC-4-286-10, U.S. Army Corps of Engineers (USACE) TM 5-691-1/2. Maintenance of Mechanical and Electrical Equipment at Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities; Systems Design Features; Recommended Maintenance Practices, USACE TM 5-810-1. Mechanical Design Heating, Ventilating, and Air Conditioning. USACE TM 5-693. Uninterruptible Power Supply System Selection, Installation, and Maintenance for Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities. USACE TM 5-691. Utility Systems Design Requirements for C4ISR Facilities.  In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p>

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

1. The assessor must verify whether procedures for each site/facility, critical systems that support operational missions require that it is heated, humidity controlled within systems specifications.
2. The assessor must verify whether procedures for systems dependent on environmental control, environmental control systems require that it has the capacity and endurance for sustained operations and reserve capacity to allow for maintenance and equipment failures.
3. The assessor must verify whether vital environmental systems have enough alternate or emergency power available to sustain mission critical systems.
4. The assessor must verify whether maintenance, technical, and operations staffs are properly trained, certified and available to operate and maintain vital environmental systems during normal, surge, and emergency operations.
5. The assessor must verify whether environmental control systems have spare parts and consumables readily available to support operations.
6. The assessor must verify whether environmental control systems supporting critical assets are fitted with fire detection, alarm, and suppression systems interlocks.
  - ◆ *It is recommended that these systems are fitted with emergency shut down devices and control features to align and secure systems to slow or prevent the spread of smoke, toxic gasses, and CBR agents.*
7. The assessor must verify whether vital assets/facilities such as command and control missions that are required to be continually operational and manned have smoke control and evacuation systems.
  - ◆ *It is recommended that ventilation should be adequately protected from the intentional or inadvertent introduction of foreign material or agents. Ventilation systems should protect and sustain personnel under likely CBR conditions. Mechanical and utility room ventilation systems should be separate from personnel systems. Waste heat systems for these facilities must be capable of supporting sustained operations regardless of the CBR protective measures implemented.*
8. The assessor must verify whether filtering and contamination control systems sufficiently protect mission critical operations and facilities from CBR agents commensurate with their missions.
9. The assessor must verify whether cooling towers and waste heat systems have sufficient normal and back up source cooling medium to support sustained vital operations.

**For Official Use Only**  
**Draft CIP FSVA Supporting Infrastructure Standards**

10. The assessor must verify that single point vulnerabilities to critical assets, missions, and facilities resulting from the collocation of environmental control systems and other utilities, and/or lack of redundancy are understood.
  - ◆ *It is recommended that measures and planning to mitigate or eliminate these vulnerabilities to include physical protection, contingency plans, procedures, installation of new and redundant systems, and physically separating vital components should be in place.*
11. The assessor must verify whether environmental control systems drawings, plans, blueprints, technical data and manuals are up to date, available, and protected from improper dissemination.
12. The assessor must verify whether vital environmental control systems have the ability to operate independently of SCADA systems.
  - ◆ *It is recommended that SCADA systems be protected and survivable. Personnel and facilities with access to SCADA systems should be properly cleared and certified.*
13. The assessor must verify whether the condition of environmental control systems meet or exceed required condition, construction, installation, and material standards for the given locality and the missions they support.
14. The assessor must verify whether contingency, disaster preparedness, continuity of operations, reconstitution, and restoration account for vital environmental control systems.
15. The assessor must verify whether vital industrial systems supporting critical missions that are dependent on environmental conditioning, cooling, and waste heat systems such cryogenic plants, compressed air and gas plants, cold storage, and refrigeration systems are sufficiently protected and survivable and if back up and/or emergency power should be available to these systems.
16. The assessor must verify whether mission assurance requirements have been considered in developing requirements for the installation, modification, and overhaul of mission critical environmental control systems.

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

**AVAILABILITY OF SUPPORTING MATERIEL AND SERVICES**

**DESCRIPTION:**

Availability of Supporting Materiel and Services includes a consideration of potential vulnerabilities inherent in the commercial support to critical assets, including supplier contractual obligations regarding the production, transport and security of materiel and services during both peacetime and periods of conflict. Attention is also paid to the ownership and control of companies providing commercial support to critical assets, especially foreign ownership/control, and the potential vulnerabilities inherent therein.

<b><u>AREA OF CONCERN:</u></b> <i>AVAILABILITY OF SUPPORTING MATERIEL AND SERVICES</i>
<b><u>TOPIC:</u></b> <i>SOURCE OF PRODUCTION</i>
<b><u>SUBTOPIC:</u></b> <i>PRODUCTION CAPABILITY</i>
<b><u>EXPLANATION:</u></b> Production Capability refers to continuous, uninterrupted production of the required level of materiel and services that support a critical asset. Vulnerabilities to disruption of a critical asset's supporting materiel and services can be reduced through the use of multiple sources of production across a wide geographic area and the ability to provide increased capacity as needed. Flexibility in capacity enables the source of materiel and services to meet increased supply requirements over an extended period. This increase in requirements may be planned or unplanned and part of the life cycle changes of the critical asset, reaction to a change in status of the critical asset or reaction to a crisis. Surge capability requires that the sources of production are able to increase supply of a product dramatically over a short period of time. Flexibility in capacity and surge capability can both be accomplished by increasing the number of sources of production, increasing production quantities at one or more of the sources of production or diverting existing production away from other consumers.
<b><u>INTENT:</u></b> To ensure that required levels of materiel and services that support the critical asset can be met and to minimize the impact to the critical asset from the loss of one or more sources of production.

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of the Production Capability of Sources of Production will include an evaluation of both the diversity and the capacity/surge capability of the sources of production. Assessment of the diversity of sources of production will examine the number of suppliers as well as the geographic diversity of the production facilities. An assessment of capacity and surge capability will examine the plans and procedures in place to ensure the adequate supply of product to the critical asset during periods of increased demand.

**CRITERIA:**

Where specific documentary sources of assessment guidelines are not identified, as in the case of Production Capability, standards for assessment are based on a variety of government and industry best practices.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. In the context of diversity, the assessor must verify the following:
  - a. The assessor will determine the degree to which the critical asset has engaged multiple suppliers for needed materiel and services. Geographical diversity of the production facilities will be emphasized to minimize the impact to the critical asset should a disruption occur that effects an entire area.
    - (1) Co-located sources of production will not be considered geographically diverse.
    - (2) Sources of production that are in close proximity to each other may be considered geographically diverse but are not as desirable as multiple sources of production that are dispersed over a broader geographic area.
  - b. The assessor will determine the degree to which the critical asset has distributed the required supply requirements among diverse sources of production to minimize the impact to the critical asset from the loss of one or more suppliers.
  - c. The assessor will determine if a mitigation strategy has been developed that will minimize the impact to the critical asset should production of the required supply be disrupted.
2. In the context of capacity the assessor must verify the following:
  - a. The assessor will determine if the critical asset has developed plans and procedures to ensure that the sources of materiel and services have sufficient flexible capacity to meet the critical asset's increased requirements.

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

- b. Plans and procedures for the implementation of increased support from the sources of supply should be reviewed annually and updated as necessary.
  - c. Mitigation strategies will be developed to minimize the impact of insufficient production capacity on continuous operation of the critical asset. Mitigation strategies should be reviewed annually and updated as needed.
3. In the context of surge capability, the assessor must verify the following:
- d. The assessor will determine if there are plans and procedures in place to ensure that there is sufficient surge capability available from the sources of production to provide adequate supplies.
  - e. Plans and procedures for the increase in materiel and services during a period of surge requirements should be reviewed annually and updated as necessary.
  - f. Mitigation strategies should be developed to ensure continuous operation of the critical asset in the event that the production sources are unable to meet surge requirements.
4. In the context of alternate sources of production the assessor must verify the following:
- a. The assessor will determine the degree to which agreements are in place between the critical asset and alternate sources of production for the production of all components necessary for the continuing operation of the critical asset. These alternate sources will be able to provide 100% coverage of the necessary products.
  - b. The assessor will determine if all necessary plans and procedures are in place to effect a seamless transition to the alternate source(s) of production. These plans and procedures will be reviewed annually and revised as necessary.
  - c. The assessor will determine if a mitigation plan has been developed. This plan should ensure that the effects to the critical asset from any disruption to the alternate sources of production are minimized. The mitigation plan will be reviewed annually and additional measures identified where possible.

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>AVAILABILITY OF SUPPORTING MATERIEL AND SERVICES</i></p>
<p><b><u>TOPIC:</u></b> <i>COMMERCIAL RELATIONSHIPS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>OWNSHIP OF SOURCES OF SUPPLY</i></p>
<p><b><u>EXPLANATION:</u></b> Ownership of Sources of Supply refers to the controlling interests of sources of supply and the degree to which those controlling interest, whether foreign or domestic, imply potential vulnerabilities for the continuous and uninterrupted operation of the critical asset. Domestic ownership refers to single or multiple owners of sources of supply and the associated degree of supply chain vulnerability. Foreign ownership refers to an examination of both the current ownership and proposed ownership, during a mergers and acquisition situation, to determine if any foreign entities own and/or control any part of a critical asset.</p>
<p><b><u>INTENT:</u></b> To ensure that the supply of materials or services that are key to the continuous operation of designated critical assets is not vulnerable to interruption due to the possible consequences of domestic or foreign ownership of the sources of production.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Ownership of Sources of Supply will include a consideration of the controlling interests of sources of supply and the degree to which those controlling interests, whether foreign or domestic, imply potential vulnerabilities for the continuous and uninterrupted operation of the critical asset. An assessment of domestic ownership of sources of supply will determine the degree of vulnerability associated with single or limited ownership of production or broader, more diverse ownership. An assessment of foreign ownership will review the current ownership, anticipated mergers and planned acquisitions to determine if foreign entities own and/or control any part of a critical asset's supply chain and the potential vulnerabilities to critical assets inherent in foreign ownership.</p>
<p><b><u>CRITERIA:</u></b> Where specific documentary sources of assessment guidelines are not identified, as in the case of Domestic Ownership of Sources of Supply, standards for assessment are based on a variety of government and industry best practices.</p>

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

The standards for assessment of Foreign Ownership of critical asset sources of supply are based on standards contained in *Department of Defense (DoD) 5220.22-M: National Industrial Security Program Operating Manual (NISPOM) (dated January 1995) incorporating Change One (July 1997) and Change Two (February 2001)*.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

1. The assessor must verify whether suppliers of materials and services that are essential to the continuous operation of the designated critical asset are owned by single or multiple domestic or foreign entities.
2. In the context of foreign ownership, the assessor must verify whether existing contractual agreements between critical assets and their suppliers include provisions to ensure uninterrupted supply of materiel or services in the event of a disruption of the supplier's primary source of production.
3. In the context of foreign ownership, the assessor must:
  - a. Verify whether or not a commercial firm that provides essential materiel or services to a critical asset is itself owned, controlled or influenced by a foreign interest as described in the *NISPOM, Chapter 2*.
  - b. Evaluate the likelihood of interruption of critical foreign-owned materials and services through analysis of factors including:
    - (1) The record of performance by the foreign owned source of supply.
    - (2) The fiscal and management stability of the foreign commercial entity that owns the key source of supply.
    - (3) The stability of the political and social environment within the foreign commercial entity's home country.
    - (4) Alignment of the economic and political interests of the foreign entity's home country and the United States (U.S.).

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>AVAILABILITY OF SUPPORTING MATERIEL AND SERVICES</i></p>
<p><b><u>TOPIC:</u></b> <i>COMMERCIAL RELATIONSHIPS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>CONTRACTOR SUPPORT OF SYSTEMS</i></p>
<p><b><u>EXPLANATION:</u></b> Contractor Support of Systems refers to an examination of the adequacy of subject matter expert (SME) support for a critical asset during both normal and surge operations.</p>
<p><b><u>INTENT:</u></b> To ensure that critical assets SME support requirements are met.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of the Contractor Support of Systems will include a consideration of critical asset SME support requirements and the capability of existing sources of subject matter support to meet those requirements. A review of the contractual agreements for contractor support will be available under all circumstances, to avoid disruption to the critical asset.</p>
<p><b><u>CRITERIA:</u></b> Where specific documentary sources of assessment guidelines are not identified, as in the case of Contractor Support of Systems, standards for assessment are based on a variety of government and industry best practices. In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify the extent to which contractual agreements ensure the availability of contractor support to the critical asset. This will include a review of the following:<ol style="list-style-type: none"><li>a. Review contracts to ensure there are provisions for providing support at an increased level for a sustained amount of time, as appropriate.</li><li>b. Ensure contracts state that background checks are conducted in accordance with the Personnel and Industrial Security standards contained in <i>NISPOM</i>.</li><li>c. Review contracts to ensure enough flexibility for situations where contractors may be directed to deploy with the critical asset or to work overtime hours.</li></ol></li></ol>

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

- |  |
|--|
| 2. The assessor must review the critical asset's contingency plans to ensure that there is redundant contractor support if needed. |
|--|

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>AVAILABILITY OF SUPPORTING MATERIEL AND SERVICES</i></p>
<p><b><u>TOPIC:</u></b> <i>COMMERCIAL RELATIONSHIPS</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>TRADING PARTNER SECURITY</i></p>
<p><b><u>EXPLANATION:</u></b> Trading Partner Security refers to the extension of security, security related information and security related training from the critical asset to suppliers of materiel and services. This includes systems or procedures that enable critical asset owners to pass appropriate security information (e.g., threat warnings, best practices, vulnerability data, etc.) along to their trading partners, and provide security training that may be helpful in reducing vulnerabilities within the supply chain.</p>
<p><b><u>INTENT:</u></b> To ensure that critical asset owners have established procedures for the sharing of security related information and training with suppliers of materiel and services.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Trading Partner Security will include a review of procedures for the sharing of security related information and training with suppliers of materiel and services.</p>
<p><b><u>CRITERIA:</u></b> The standard for the assessment of Trading Partner Security is based on the guidelines contained in the <i>Asia-Pacific Economic Cooperation (APEC) Private Sector Supply Chain Security Guidelines (undated)</i>. This reference addresses the supplemented as required and indicated below.</p> <p>In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p> <ol style="list-style-type: none"><li>1. The assessor must verify the extent to which critical assets owners are aware of the security procedures and associated security training conducted by supply chain partners.</li><li>2. The assessor must verify the extent to which critical asset owners have communication plans established that facilitate the exchange of security related information between their trading partners/suppliers/contractors. This information may include vulnerability alerts, threat warnings and other information that may affect the security of elements of the supply chain.</li></ol>

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

**AREA OF CONCERN:**

*AVAILABILITY OF SUPPORTING MATERIEL AND SERVICES*

**TOPIC:**

*TRANSIT*

**SUBTOPIC:**

*TRANSPORT CAPABILITY*

**EXPLANATION:**

Transport Capability refers to the use of a variety of transportation resources. Vulnerabilities to disruption of a critical asset's transportation capability can be reduced by ensuring diversity, capacity, surge capability and alternate transportation resources. Diversity describes the use of multiple modes of transportation (e.g., multiple modes such as rail, truck, air, etc.). It also includes redundancy in each mode of transportation (e.g., airlines, truck companies to transport suppliers, etc.) for the supply of a critical asset. Capacity refers to the ability to provide a moderately increased transportation capability for an extended period of time, while surge capability requires that the transportation resources are able to increase dramatically over a short period of time. Alternate transportation resources refer to those plans and procedures that exist to ensure that no interruption in service or operation occurs if the primary transportation source for suppliers to a critical asset is disrupted.

**INTENT:**

To ensure that the required levels of transport are available to move goods through the supply chain in order to preclude disruption to a critical asset.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of Transport Capability will include a review of the diversity, capacity, and surge capability and alternate sources of the transportation resources used to supply a critical asset. An assessment of the diversity of transport capability will include a review of the number of modes of transportation as well as redundancy in those modes. An assessment of capacity, surge capability and alternate sources of transportation will examine the plans and procedures in place to ensure the adequate transport of goods to the critical asset during periods of increased demand.

**CRITERIA:**

Where specific documentary sources of assessment guidelines are not identified, as in the case of Transport Capability, standards for assessment are based on a variety of government and industry best practices.

In support of a given mission and where applicable, the FSIVA assessor must verify the following:

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

1. In the context of diversity the assessor must verify the following:
  - a. The assessor will verify that there are multiple modes of transportation for needed supplies, as well as redundancy for each mode of transportation.
  - b. The assessor will verify that the transportation resources are distributed to minimize the impact of the loss of a single transportation mode.
  - c. The assessor will verify that a mitigation strategy exists to minimize the impact to the critical asset should transport of required supplies be disrupted or if transportation resources are not adequate to prevent disruption to the critical asset. Mitigation strategies will be reviewed annually.
2. In the context of capacity, the assessor must verify the following:
  - a. The assessor will review plans and procedures to ensure that there is sufficient transport capacity available to provide adequate supplies during a crisis.
  - b. The assessor will verify that plans and procedures for ensuring transport capacity are reviewed annually.
  - c. The assessor will verify that mitigation strategies exist to minimize the impact on the critical asset in the event that the transport capacity is not adequate to sustain supplies to the critical asset. Mitigation strategies will be reviewed annually.
3. In the context of surge capacity, the assessor must verify the following:
  - a. The assessor will review the plans and procedures for ensuring that there is sufficient surge capability available from the transportation resources to provide adequate supplies in the event that a surge in transportation is required.
  - b. The assessor will verify that plans and procedures for ensuring adequate transportation resources are available to meet surge requirements will be reviewed annually.
  - c. The assessor will verify that mitigation strategies exist to ensure continuous operation of the critical asset in the event that the transportation resources are unable to meet surge requirements. Mitigation plans will be reviewed annually.
4. In the context of alternate transportation resources, the assessor must verify the following:

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

- a. The assessor will verify that plans and procedures exist to ensure a seamless transition to alternate transportation resources. These plans and procedures will be reviewed annually and revised as necessary. A variety of transportation solutions (e.g., modes, routes, sources, etc.) will be emphasized as the norm rather than the exception.
- b. The assessor will review the plans and procedures to ensure that alternate sources of transportation are available for all components necessary for the continuing operation of the critical asset, in the event that the primary transportation resource is not available. These alternate sources will be able to provide 100% coverage of the necessary supplies needed.
- c. The assessor will verify that mitigation plans exist for use in the event that a redundant or alternate source of transportation is not available. These plans will ensure that the effects to the critical asset from the mitigation plan will be reviewed annually and additional measures identified where possible.

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>AVAILABILITY OF SUPPORTING MATERIEL AND SERVICES</i></p>
<p><b><u>TOPIC:</u></b> <i>TRANSIT</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>CONVEYANCE AND PROCEDURAL SECURITY</i></p>
<p><b><u>EXPLANATION:</u></b> Conveyance and Procedural Security refers to protecting against the introduction of unauthorized personnel and materiel into the critical asset's supply chain, and to assure the locations of goods in the supply chain are recorded and in verifiable locations.</p>
<p><b><u>INTENT:</u></b> To ensure the continuous operation of the critical asset by precluding events related to the introduction of unauthorized personnel or materiel into the supply chain or impeded movement of goods through the supply chain.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of Conveyance and Procedural Security will include a review of the critical asset's procedures for receiving supplies to ensure that unauthorized materiel or personnel have not been injected into the supply chain, detection and reporting/notification procedures for suspicious activity, and the measures taken to secure supplies in transit to a critical asset. Contractual agreements will also be reviewed to ensure that there are documented procedures for recording and verifying the location and security of goods in the supply chain.</p>
<p><b><u>CRITERIA:</u></b> The standards for the assessment of Conveyance and Procedural Security are based on the guidelines contained in the <i>Asia-Pacific Economic Cooperation (APEC) Private Sector Supply Chain Security Guidelines (undated)</i> and the <i>U.S. Customs Customs-Trade Partnership Against Terrorism (C-TPAT) Guidelines (undated)</i>. These references address the required areas for assessment of this subtopic. The baseline references are supplemented as required and as indicated below.  In support of a given mission and where applicable, the FSIVA assessor must verify the following:</p>

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

1. In the context of procedural security the assessor must verify the following:
  - a. The assessor will review the procedures for receiving supplies at the critical asset to ensure that unauthorized material or personnel have not been injected into the supply chain. The following will be reviewed as appropriate:
    - (1) Procedures for recording and verifying removal of goods from the supply chain.
    - (2) Procedures for protection against unmanifested material being introduced to the critical asset. The review will include procedures for affixing, recording, tracking and verifying tamper-proof/non-counterfeitable seals on containers and trailers. It will also ensure that seals are not used in strict numeric sequence. In addition, procedures for verifying proper marking, weighing, counting and documenting of cargo/equipment, verified against manifest documents will be included.
    - (3) Procedures for storing empty and full containers to prevent unauthorized access, including the use of tamper-proof/non-counterfeitable seals, as well as procedures for checking empty containers received for storage or loading to assure their structure has been modified.
    - (4) Procedures for verifying the identity and authority of the carrier requesting delivery of cargo prior to cargo release.
    - (5) Procedures for random, unannounced security assessments and inspection of persons and packages.
  - b. The assessor will verify that the critical asset owners have detection and reporting/notification procedures for suspicious activity (e.g., shortages, overages, irregularity or illegal activities) relating to the supplies received. These procedures will cover notification to other critical assets, suppliers, customs and law enforcement, etc.
  - c. The assessor will review contracts with suppliers and transporters to ensure that there are documented procedures for recording, verifying and tracking the timely movement and quantities of incoming goods.
2. In the context of conveyance security the assessor must verify the following:
  - a. Conveyance security refers to the measures taken to secure the mode of delivery of supply to a critical asset. Critical asset owners may not have direct authority over the procedures taken during transit; however, assessor must verify owners make every effort to ensure the security of the supplies while in transit.

**For Official Use Only**  
**Draft CIP FSVA Supporting Materiel and Services Standards**

- b. The assessor will review the following areas, as applicable:
- (1) Plans, procedures, or criteria established by the critical asset owners that address the requirements for conveyance security of the goods delivered to the critical asset.
  - (2) Procedures for reporting instances in which unauthorized personnel, unmanifested materials or signs of tampering of a conveyance are discovered.
  - (3) The assessor will review contracts with suppliers and transporters to verify that there are documented procedures to ensure security of supplies in transit, such as procedures for the use of transponders for continually tracking conveyances, or of automatic electronic transmittal of smart card data to U.S. Customs, if available.

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

**DTRA-RECOMMENDED WEAPONS OF MASS DESTRUCTION**

<p><b><u>AREA OF CONCERN:</u></b></p> <p><i>WEAPONS OF MASS DESTRUCTION (WMD) VULNERABILITY ASSESSMENT AND ANALYSIS</i></p>
<p><b><u>TOPIC:</u></b></p> <p><i>WMD RESPONSE</i></p>
<p><b><u>SUBTOPIC:</u></b></p> <p><i>N/AWMD RESPONSE – INITIAL ACTIONS/RECOVERY/CONTINUITY OF OPERATIONS (COOP)</i></p>
<p><b><u>EXPLANATION:</u></b></p> <p>Assessment of WMD post-attack capabilities. Focus is on internal and external casualty care and mission continuity. Alternate operations centers (AOC) and plans, personnel, and procedures to support the activation and operation of the AOC are assessed.</p>
<p><b><u>INTENT:</u></b></p> <p>To assess the site’s ability to accomplish the assigned missions either through decontamination/casualty care or the implementation of COOP plans. Evaluates requirements and plans to continue the mission after a CBR attack.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b></p> <p>An assessment of this area will include review of all plans, procedures, equipment, training, and capabilities related to internal and external immediate and mission continuity response to a WMD attack or HAZMAT release.</p>
<p><b><u>RESPONDERS:</u></b></p> <ol style="list-style-type: none"><li>1. Designated response agencies should be equipped with sufficient equipment, both type and quantity, to provide for effective execution of prescribed duties and to assure effective response to emergencies. Equipment should include the properly equipped vehicles and PPE.</li><li>2. Assess the access (response time and restricted zone entry), detection, and protection assets of the primary and follow-on incident responders similar to site assessment of the same assets.</li><li>3. Determine if specialized capabilities (burn units, EOD, Urban Search and Rescue Teams, CST, etc.) that might have application for WMD casualties are available in the area and if the site is aware and has plans and procedures in place to rapidly avail itself of these resources.</li></ol>

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

4. Determine if regionally based assets are likely to be available to the site of if they have national or global commitments or are frequently deployed outside the region.
5. Assess the degree of integration of the site and civil portions concerning the command of on-scene incidents. Communications networks and response structure should likely follow Fire and Rescue Incident Command System (ICS) procedures. Deviations from this national response norm must be explored.
6. Communications equipment should provide interoperability between various local/state/federal, and host nation organizations.

**DECONTAMINATION:**

1. The installation should be capable of establishing both gross and technical decontamination stations for the responders as well as the decontamination of personnel and key equipment.
2. When augmentation personnel are required for specific duties such as first-aid, triage, decontamination, and transportation of casualties, they must be trained and exercised in these duties; exercises should be integrated with internal and external response organizations.
3. Assess the decontamination of casualties, particularly at the medical treatment facility. Proper confirmation of decontamination using detectors is crucial to preventing the contamination of the health care workers, facilities, and equipment.
4. If decontamination solutions (including water) are used, assess the training and procedures employed to prevent damage to critical systems.
5. Assess containment, storage, and disposal procedures for decontamination solutions, before and after usage.

**CONTINUITY OF OPERATIONS PLANS (COOP)**

1. The assessment of COOP is primarily a review of the plans and procedures and their relevance and feasibility in a CBR environment.
2. If the COOP site is assessed then the AOC assessment follows the normal assessment protocol with the following exceptions:
  - a. Determine if personnel from the primary site will be required for manning at the COOP site, thereby requiring decontamination, contamination containment, entry / exit procedures and detection capabilities at the AOC or enroute.

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

- b. Determine the intent for the AOC. Duration and durability of the AOCs varies greatly and capabilities must be assessed with the Concept of Operations (ConOps) for the AOC in mind. Once the ConOps is known the applicable assessment parameters for CBR preparedness and contamination avoidance mirror those of the primary site.

**RECOVERY/RECONSTITUTION:**

1. A CBR contaminated site may take months or years to decontaminate and be able to be reoccupied or it may never be possible (radiological in particular). Is there any indication (COOP plans, dispersal of mission tasks, available space/assets in the area) that this has been addressed, even if only in discussions of senior leaders?
2. Assess the ability to reconstitute the mission, by relocation, decontamination, or replacement of assets should a site be contaminated and unusable.
3. Capabilities and assets should be prioritized for reconstitution. This prioritized list should be reviewed for completeness and coherence.

**BEST PRACTICES/INDUSTRY STANDARDS/REFERENCES:**

FM 3-5, NBC Decontamination

FM 4-02.7 "Health Service Support in a NBC Environment, 1 OCT 2002

AFH 32-4001, "USAF Ability to Survive and Operate Procedures in a NBC Environment," Vol 4, 1 MAR 1998

AFH 32-4004, "Emergency Response Operations," 1 DEC 1995

AFH 32-4014, "Operations in a Chemical and Biological Warfare Environment," Vol 2, Dec 1997

STANAG 2103, "Reporting Nuclear Detonations, Biological and Chemical Attacks, and Predicting the Warning of Associated Hazards and Hazard Areas," 1 Jul 2001

DOT, Emergency Response Guidebook 2000

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

**AREA OF CONCERN:**

*WEAPONS OF MASS DESTRUCTION (WMD)  
VULNERABILITY ASSESSMENT AND ANALYSIS*

**TOPIC:**

*WMD AVOIDANCE AND RESPONSE*

**SUBTOPIC:**

*WMD RESPONSE - WMD AVOIDANCE*

**EXPLANATION:**

Focus is on internal and external threat detection, alarms and notification measures, and implementation of actions to reduce contamination of personnel, facilities, and equipment. Both passive measures (quantity, location and susceptibility of critical assets to CBR attack) and active measures (detection, warning and protection) will be assessed.

**INTENT:**

To ensure organization has fully surveyed the site's CBR avoidance measures and capability to protect mission essential equipment, personnel and facilities from contamination.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of this area includes a survey of internal and external WMD/HAZMAT response resources, identification of relevant shortfalls in capability, and plans/procedures implemented upon hazard identification. The assessment includes:

**PASSIVE AVOIDANCE MEASURES:**

1. Assess potential agent entry points (air intakes, vents, windows/doors, loading docks, mailroom, water, food) and review structural, mechanical, or delivery modifications that are or might be implemented to reduce the uptake of agent.
2. Determine the effectiveness of physical security or procedural actions (particularly access control measures) enacted at each threat level to prevent the entry of agent directly into a facility (i.e. mechanical rooms, HVAC air intakes, mailrooms).
3. Evaluate dispersion or separation of critical assets; alternate operations facilities; covering, concealment, or other denial/deception methods used to reduce contamination of assets and degrade mission.
4. Assess perimeter surveillance and security: particularly potential upwind release points and programmed measures to increase security presence and surveillance beyond the site boundaries during times of increased threat.

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

5. Examine HVAC actions, shelter in place and evacuation SOPs and checklists. Interview parties responsible for initiation of actions to determine the level of understanding, authority and communication required of each action. Determine if the measures have ever been tested and the frequency of exercises.

**ACTIVE AVOIDANCE MEASURES:**

1. Detection:
  - a. Assess the adequacy of detection equipment to meet CBR threats as well as likely HAZMAT incidents.
    - (1) Start-up time, response time, sensitivity, selectivity, interferences, alarm capability, power requirements, portability, durability, operator requirements.
    - (2) Capability to test water, food, vapors, liquids, powders, dusty agents.
    - (3) Assess capability to provide both standoff and point detection.
  - b. Determine procedures for employing detection equipment: (i.e. positioning, sampling frequency or continuous monitoring, meteorological inputs).
  - c. Determine maintenance and storage protocols for detection equipment. Assess tracking for shelf-life items, periodic inspections/calibration/maintenance actions.
  - d. Determine additional detection assets available to the site and timeliness of their arrival on site after a release (CBIRF, TEU, CBIAC, WMD-CST, etc).
  - e. Assess operator training, proficiency, and awareness of detection capabilities, shortfalls, and operator pitfalls.
  - f. Assess the ability to generate dispersion or hazard prediction models. Evaluate access to meteorological and release data and the ability to request or receive inputs necessary for valid modeling (i.e. release volumes, terrain, ground and low altitude weather) in a timely and useful format.
  - g. Assess the dispersion model's capabilities for predicting CBR (particularly warfare agents) hazards. Determine training and proficiency of dispersion modelers. If modeling is conducted off site, evaluate the validity of the models, sources and fidelity of input data, response time to the facility, security and reliability of communication links to the facility.
2. Notification:
  - a. Assess alarms, public address systems and announcements effectiveness in warning personnel and clearly directing protective actions.

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

- b. Assess effectiveness of evacuation or shelter-in-place procedures, accountability, and post-attack actions (building purging, decontamination, casualty response) in limiting exposure of personnel to agents.
- 3. Personal Protection:
  - a. Personal Protective Equipment (PPE):
    - (1) Availability to mission essential personnel and security forces
    - (2) Fitting, training, inspection, storage, tracking of shelf-life items
    - (3) Impact on conducting mission-essential functions
  - b. Immunization currency of essential personnel
  - c. Availability and serviceability of antidotes, prophylactic drugs, lotions, or other personnel protective measures
- 4. Collective Protection:
  - a. Passive (unpressured) collective protection: Assess adequacy of weather sealing, ventilation system and its configuration and operational capabilities. Determine the location of air intakes and the building's mechanical spaces. Assess security and access control measures and project vulnerabilities of mechanical spaces /HVAC system/filtration system to contamination.
    - (1) Ensure shelter-in-place location have been identified. Shelter procedures, supplies and ventilation should exceed requirements for anticipated demands for sheltering time/occupancy.
    - (2) Critical utilities should be supported by back-up power systems.
    - (3) Assess HVAC maintenance and operation schedules. If rapid shutdown or purge capabilities exist evaluate these capabilities and ensure plans adequately address the use of these systems. Assess the access to HVAC system controls (mechanical spaces, off site SCADA, contractual, EOC).
    - (4) Determine CBR filter efficiency and effectiveness against expected threats.
  - b. Active (positive pressure) collective protection (CP):
    - (1) Review the operating procedures for the CP equipment/system. Is the CP operational all the time? If not what is the procedure and time needed to provide a protected environment?
    - (2) Assess the entire active collective protection system. Is it integrated with the HVAC system, what is the replacement schedule for filters? How often is the system tested? What is the availability of replacement parts?

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

- (3) Review Toxic Free Air (TFA) and Contamination Containment Areas (CCA) for procedures, maintenance, capabilities and leak testing.

**BEST PRACTICES/INDUSTRY STANDARDS/REFERENCES:**

Joint Service Nuclear, Biological, and Chemical Defense Concept, Sep 1997

U.S. Army Field Manual (FM) 3-3, "Chemical and Biological Contamination Avoidance," 16 NOV 92

U.S. Army Corps of Engineers Technical Instruction 853-01, *Protecting Buildings and Their Occupants from Airborne Hazards*

FM 3-3-1, "Nuclear Contamination Avoidance," 9 SEP 94

FM 3-4, "NBC Protection," 29 MAY 92

AFMAN 32-4005, "Personnel Protection and Attack Actions," 1 Mar 1999

FN 3-4-1, "Multi-service Procedures for NBC Defense of Fixed Sites, Ports, and Airfields," 7 NOV 97

Engineer Technical Letter 1110-3-498, "Design of Collective Protection Shelters to Resist CBR Agents," 24 FEB 99

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>WEAPONS OF MASS DESTRUCTION (WMD)</i></p>
<p><b><u>TOPIC:</u></b> <i>CHEMICAL, BIOLOGICAL, AND RADIOLOGICAL</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>WMD PREPAREDNESS</i></p>
<p><b><u>EXPLANATION:</u></b> Airborne CBR attacks can be standoff, external but proximate, or internal to the intended targeted facility or location. In addition to airborne dissemination CBR agents can be delivered via mail, food, and water as well. The farther a CBR release is from the intended target the more the effectiveness of the attack depends on quantity and favorable meteorological conditions and the more susceptible it is to detection and protective actions. Vulnerabilities and corresponding mitigation measures are therefore often standoff issues designed to force attackers into less effective standoff attack parameters.</p>
<p><b><u>INTENT:</u></b> To ensure mission critical assets (personnel, equipment, and facilities) are protected in the event of a CBR attack and provide mitigation measures to reduce the likelihood or effectiveness of a CBR attack. In an attempt to reduce the CBR threat to the mission, special attention is directed at readily exploitable vulnerabilities or particularly vulnerable mission assets.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of this includes a review of CBR agents (military WMD agents and toxic industrial materials (TIMs) manufactured, transported or stored in sufficient quantity to cause mass casualties if released intentionally or accidentally) that could affect mission continuity. Assessment includes not only releases capable of producing mass casualties but also contamination that could degrade or deny missions by closing of facilities and/or loss of use of essential equipment for long periods of time.</p>

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

**AREA OF CONCERN:**

*WEAPONS OF MASS DESTRUCTION (WMD)*

**TOPIC:**

**SUBTOPIC:**

*WMD PREPAREDNESS – PLANS AND TRAINING*

**EXPLANATION:**

Focus is on threat assessment and awareness of vulnerabilities and likely attack avenues, disaster plans, training in response and protective actions, and contingency plans for mission interruption.

**INTENT:**

To ensure awareness of WMD threats is reflected in plans and training and efforts to protect the facility, personnel and mission include WMD attack/HAZMAT release scenarios and responses.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of this area includes a review of WMD/HAZMAT programs and all plans, training, and exercises related to WMD preparedness, response, and COOPs.

**THREAT/CONTAMINATION FACTORS:**

1. Consider the political, military, or symbolic significance of the site and Chemical, Biological, and Radiological (CBR) capabilities of known opposition groups.
2. Review national, regional and local threat documents and interview security and intelligence managers on assessment of foreign and domestic WMD threats.
3. Interview local authorities (police, emergency responders and planners) on industrial or agricultural HAZardous MATerials (HAZMAT) sites, methamphetamine production, extremist or criminal activities that could pose a WMD threat to the site.
4. Determine the locations of major HAZMAT (Tier 1 chemicals) producers or storage sites in the vicinity of the site.
5. Investigate all transportation routes (rail, road, water, and air) for proximity and types and quantities of HAZMAT commonly conveyed.
6. Determine prevailing and/or seasonal meteorological conditions and assess the impact on the site's vulnerability to HAZMAT sites and transportation routes

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

7. Develop an analysis of the minimum quantities of CBR agents or HAZMAT necessary to neutralize critical facilities based on probable standoff, proximal or internal attack scenarios.
8. Evaluate deliveries (mail, packages, food, water) for the potential to introduce agents into the facilities. Observe location, inspection procedures and volume of material processed into the site and determine feasibility of agent introduction.
9. Evaluate location and structure of critical assets: elevation, concealment from view, type of construction, public access, surrounding buildings/industries

**PLANNING:**

1. Assess CBR Standard Operating Procedures (SOPs) effectiveness in protecting against a wide range of general CBR/HAZMAT threats.
2. Assess plans and mitigation measures for combating specific regional and local organization's CBR capabilities that pose a threat to the site.
3. Ensure plans and SOP reflect existing CBR capabilities (detection, alarms, protection) and are realistic regarding operational expectations.
4. Review any plume or release scenarios that have been developed to focus training, plans or other allocation of resources.
5. The CBR defense plan should be a comprehensive appendix to the Anti-Terrorist/Force Protection (AT/FP) Plan. It should include: CBR agent and other information and planning, communications, legal, CBR defense, security, firefighting, health services support, resource support, mass casualty management, decontamination procedures, and host nation or national support functions..
6. Review FPCON, DEFCON, and (AT/FP) guidance for specific CBR protective or increased preparedness measures.
7. Assess integration of external response forces into CBR response plans; are there mutual aid/assistance agreements verifying responsibilities for response and recovery?
8. Do plans address nonmilitary civil servants, essential contractors, or key foreign national workers issues? Will PPE be provided to these people or identify and train military members (with PPE) to cover their essential tasks during attacks.
9. Plans must address evacuation routes and shelter in place locations and actions. Evacuation in particular must be site, agent, and scenario specific but broad guidelines capable of being tailored for a wide range of likely threats should be in place.

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

10. CBR plan should identify an Emergency Operations Center (EOC) and an alternate EOC, either a fixed site or preferably a mobile command post that can be located near the incident.
11. Plans must address work/rest cycles for individuals working in PPE, prophylaxis measures, and individual response actions.

**TRAINING/EXERCISES:**

1. Assess individual and collective response/protection proficiency.
  - a. Operation, awareness, and documented or observed response to alarms
  - b. Immediate and follow-on casualty care and transport of patients
  - c. Contamination control and decontamination procedures
2. Assess training for personnel tasked to operate CBR detection equipment.
3. Exercises must develop realistic CBR decision-making and support the development and use of decision support tools. Review training aids and CBR awareness/response guides or checklists for accuracy, completeness, and effectiveness.
4. Inclusion of external and internal response assets in exercises, focus on access and involvement of key mission centers and personnel.
5. Frequency and variety of CBR exercises: emphasis on mission continuity and realism in work, casualty care, and contamination avoidance are important issues.
6. Exercises should be used to evaluate the state of CBR readiness. Assess the standards or criterion are used to rate readiness. Review after-action reports and look for the incorporation of "lessons learned" into procedures, training, and future exercises.
7. Personal Protective Equipment (PPE) fitting, training, and tracking for recall or shelf-life expiration.

**BEST PRACTICES/INDUSTRY STANDARDS/REFERENCES:**

FM 3-11.14, "Multiservice Tactics, Techniques and Procedures for Nuclear, Biological and Chemical (NBC) Vulnerability Assessment," Draft June 2003  
DOD Instruction 2000.16, "DOD Combating Terrorism Program Standards," 15 SEP 96  
WMD Appendix, AT/FP Installation Planning Template, J34, 1 NOV 98  
JP 3-10.1, "Joint Tactics, Techniques, and Procedures for Base Defense." 23 July 1996  
JP 3-11, "Joint Doctrine for Nuclear, Biological, and Chemical Environments," 11 July 2000

**For Official Use Only**  
**DTRA-Recommended Weapons of Mass Destruction Standards**

AF Handbook 32-4014, V 1-4, "USAF Operations in a Chemical and Biological Warfare Environment," 1 MAR 99

AF Handbook 10-2502, "USAF Weapons of Mass Destruction Threat Planning and Response"

AF Manual 32-4017, "Civil Engineer Readiness Technician's Manual for Nuclear, Biological, and Chemical Defense," 1 JUN 98

Department of Health and Human Services Publication 2002-139, *Guidance for Protecting Building Environments from Airborne Chemical, Biological and Radiological Attacks*

Lawrence Berkeley National Laboratory Pub 51959, *Protecting Buildings from a Biological or Chemical Release*

FM 3-14, "NBC Vulnerability Analysis," 12 NOV 97

Unified Facilities Criteria 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*

DODD 2000.12, DOD Antiterrorism/Force Protection (AT/FP) Program, 13 April 1999

DODI 2000.16, DOD Antiterrorism Standards, 14 June 2001

AFH 32-4014, "USAF Operation in a Chemical and Biological Warfare Environment, Planning and Analysis," Vol 1, Mar 1998

FM 3-11, "Multiservice Tactics, Techniques and Procedures for NBC Defense Operations," June 2002

AFMAN 10-2602, "Nuclear, Biological, Chemical and Conventional (NBCC) Defense Operations and Standards"

OPNAV P-86-1-95, "US Navy CBR Defense/US Marine Corps NBC Defense Handbook," Apr 1995

STANAG 2133 (SD6), "Vulnerability Analysis of Chemical and Biological Hazards

STANAG 2353, NBC (Editions) - "Evaluation of NBC Defense Capability," 24b Mar 2000

STANAG 2984, "Graduated Levels of NBC Threat and Associated Protection, 21 Mar 2001

CBIAC Chemical, Biological, and Radiological Threat, Vulnerability, and Protection Assessment, 7 Dec 2001

FEMA Manual 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, May 2003

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

**DTRA-RECOMMENDED EMERGENCY OPERATIONS**

Emergency Operations refers to planning, material and training issues related to the development of disaster preparedness/emergency management and business continuity plans; threat and hazard identification; mitigation; emergency response both internal and external; and damage control, recovery and continuity of operations.

Having a separate area of concern for Emergency Operations rather than merely touching on selected aspects of emergency planning in several areas (Plans, Consequence Mgt & Safety) gives coherence to emergency preparedness, response, and mission continuity issues.

<b><u>AREA OF CONCERN:</u></b> <i>EMERGENCY OPERATIONS</i>
<b><u>TOPIC:</u></b> <i>DAMAGE CONTROL AND RECOVERY</i>
<b><u>SUBTOPIC:</u></b> <i>CONTINUITY OF OPERATIONS (COOP)</i>
<b><u>EXPLANATION:</u></b> Continuity of Operations (COOP) refers to the program supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure capability to continue mission essential functions and services through personnel training, plan testing, and maintenance.
<b><u>INTENT:</u></b> To ensure an effective program is in place to plan, prepare for, and respond to interruptions in mission essential functions and services.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of this area will include a review of COOP, and the training, exercises, resources, command and control capabilities necessary to implement the plans.
<b><u>BEST PRACTICES/INDUSTRY STANDARDS:</u></b> Standards for the assessment of Emergency Operations were derived from the following:  Federal Emergency Management Agency (FEMA). Emergency management in the United States is by function and by law a cooperative effort on the part of all levels of government and the private sector. Within the Federal Government, FEMA serves as

## For Official Use Only

### DTRA-Recommended Emergency Operations Standards

the lead agency for civil defense and coordinates with other federal agencies with responsibilities or capabilities valuable to national security emergency preparedness. Various FEMA publications and training courses are useful references.

Federal Emergency Management Agency (FEMA), "Guide for All-Hazard Emergency Operations Planning, State and Local Guide (101)"The Federal Response Plan

Federal Regulations:

40 CFR 355 Emergency Planning and Community Right to Know Act

40 CFR 68 Risk Management Programs

29 CFR 1910.38 Employee Emergency Plans and Fire Prevention Plans

PDD 67. Continuity of Operations

Federal Preparedness Circular (FPC) 65. Federal Executive Branch Continuity of Operations (COOP)

DoD Directive 3020.6. Assignment of National Security Emergency Preparedness Responsibilities to DoD Components

DoDI 6055.6. DoD Fire and Emergency Services Program

DoDI 2000.16. DoD Antiterrorism Standards

DoDI 2000.18. DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines

UFC 3-600-01 Fire Protection for Facilities Engineering, Design and Construction.

Department of Transportation " 2000 Emergency Response Handbook, A Guide for First Responders"

National Fire Protection Association (NFPA). The NFPA coordinates the development of various codes to promote and enhance fire prevention, life safety and emergency response. A number of NFPA codes directly pertain to emergency preparedness and response.

NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs.

To meet mission assurance requirements for Continuity of Operations, the cognizant authority should have a Continuity of Operations Program that adequately captures the requirements and relevant recommendations from the references listed above. The assessor should review the program giving consideration to the following criteria:

1. COOP program objectives are clearly stated, supported and financed by management, and understood by employees. The COOP program should:
  - a. Ensure the continuous performance of an asset's essential functions/ operations during an emergency.
  - b. Protect essential facilities, equipment, records, and other assets.
  - c. Reduce or mitigate disruptions to operations.
  - d. Reduce loss of life; minimize damage losses.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

- e. Achieve a timely and orderly recovery from an emergency and resumption of full service to customers.
  - f. Include procedures for a periodic comprehensive self-assessment of the program elements listed below.
2. The COOP must:
- a. Be maintained at a high level of readiness.
  - b. Designate a COOP program manager and alternate.
  - c. Be capable of implementation both with and without warning.
  - d. Take maximum advantage of existing infrastructures.
  - e. Be included in the asset long-range strategic and program management plan to ensure sufficient resources are maintained to support the COOP.
3. A viable COOP program addresses the following elements:
- a. Plans and Procedures
    - (1) Delineate essential functions, applications, processes, equipment, and activities.
    - (2) Outline a decision process for implementing the COOP.
    - (3) Establish a roster of fully equipped and trained emergency personnel with the authority to perform essential functions and activities.
    - (4) Include procedures for employee advisories and alerts, instructions for relocating to pre-designated facilities, with and without warning, during duty and non-duty hours.
    - (5) Establish reliable processes and procedures for acquiring resources necessary to continue essential functions and sustain operations for up to 30 days.
  - b. Identification of Essential Functions, Applications, Processes, and Equipment
    - (1) Identify and prioritize essential functions, processes and equipment.
    - (2) Establish staffing and resource requirements.
    - (3) Identify mission-critical data and systems.
    - (4) Integrate supporting activities to ensure efficiency of operations.
  - c. Delegations of Authority
    - (1) Identify programs and administrative authorities needed for effective operations.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

- (2) Identify the circumstances under which the authorities would be exercised.
  - (3) Document the authorities at all points where emergency actions may be required.
  - (4) State explicitly the authority of designated successors.
  - (5) Ensure officials who may be required to assume authorities are trained to carry out emergency duties.
- d. Orders of Succession
- (1) Establish an order of succession.
  - (2) Identify any limitations of authority of successors.
  - (3) Include in succession procedures the conditions under which succession would take place.
- e. Alternate Facilities Should Provide:
- (1) Immediate capability to perform essential functions.
  - (2) Sufficient space and equipment to sustain the relocating organization.
  - (3) Interoperable communications.
  - (4) Reliable logistical support.
  - (5) Ability to sustain operations for up to 30 days.
  - (6) Appropriate physical security and access controls.
- f. Vital Records and Databases
- (1) Emergency operating records
  - (2) Legal and financial records
- g. Tests, Training, and Exercises
- (1) Individual and team training
  - (2) Internal asset testing of COOP
  - (3) Testing of alert procedures
  - (4) Refresher orientation
  - (5) Joint agency exercises
- h. Reconstitution
- (1) Procedures and timelines for returning the asset to primary facilities and normal operations.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

<p><b><u>AREA OF CONCERN:</u></b>  <i>EMERGENCY OPERATIONS</i></p>
<p><b><u>TOPIC:</u></b>  <i>DAMAGE CONTROL AND RECOVERY</i></p>
<p><b><u>SUBTOPIC:</u></b>  <i>DAMAGE CONTROL AND RECOVERY</i></p>
<p><b><u>EXPLANATION:</u></b>            Damage control and recovery refers to measures taken in response to an incident to contain and control immediate damage, prolong effective continuation of the mission, ensure an orderly transfer of mission essential functions and services to an alternate site, recover from the incident, and reconstitute full mission capabilities.</p>
<p><b><u>INTENT:</u></b>            To ensure that mission continuity remains the top priority during any emergencies.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b>            An assessment of this area will review plans, equipment, exercises, and training related to an organization’s ability to control damage, recover from an emergency incident, and continue or transfer and reconstitute mission essential functions and services during and following an emergency incident.</p>
<p><b><u>BEST PRACTICES/INDUSTRY STANDARDS:</u></b>            Standards for the assessment of Emergency Operations were derived from the following:            Federal Emergency Management Agency (FEMA). Emergency management in the United States is by function and by law a cooperative effort on the part of all levels of government and the private sector. Within the Federal Government, FEMA serves as the lead agency for civil defense and coordinates with other federal agencies with responsibilities or capabilities valuable to national security emergency preparedness. Various FEMA publications and training courses are useful references.</p>
<p>Federal Emergency Management Agency (FEMA), “Guide for All-Hazard Emergency Operations Planning, State and Local Guide (101)”            The Federal Response Plan            Federal Regulations:                40 CFR 355 Emergency Planning and Community Right to Know Act                40 CFR 68 Risk Management Programs                29 CFR 1910.38 Employee Emergency Plans and Fire Prevention Plans            PDD 67. Continuity of Operations</p>

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

Federal Preparedness Circular (FPC) 65. Federal Executive Branch Continuity of Operations (COOP)

DoD Directive 3020.6. Assignment of National Security Emergency Preparedness Responsibilities to DoD Components

DoDI 6055.6. DoD Fire and Emergency Services Program

DoDI 2000.16. DoD Antiterrorism Standards

DoDI 2000.18. DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines

UFC 3-600-01 Fire Protection for Facilities Engineering, Design and Construction. Department of Transportation “ 2000 Emergency Response Handbook, A Guide for First Responders”

National Fire Protection Association (NFPA). The NFPA coordinates the development of various codes to promote and enhance fire prevention, life safety and emergency response. A number of NFPA codes directly pertain to emergency preparedness and response.

To meet mission assurance requirements for Damage Control and Recovery, the cognizant authority must address the following best practices:

1. The asset has a designated Disaster Preparedness Officer and a Disaster Preparedness Plan that is fully coordinated with Emergency Management and Continuity of Operations Plans that may also exist.
2. Cognizant authority has determined desirable immediate actions that employees should take in response to foreseeable emergencies.
3. Occupant Emergency Plans identify key personnel, their responsibilities and roles, and the reporting and other immediate actions related to fire fighting or other damage control efforts that employees are expected to take.
4. Appropriate damage control equipment has been located close to critical mission areas. Requirements will vary from facility to facility but should be appropriate to facilitate temporary repairs and to promote mission continuity. This equipment might include pre-stocked spare parts, medical equipment, Personal Protective Equipment, materials to prevent flooding or other water intrusion, flashlights, batteries, emergency water and food supplies, etc.
5. Appropriate portable fire fighting equipment is installed in critical facilities and employees have been trained in the use of the equipment.
6. Recovery plans establish command and control organization and priorities/procedures for damage assessment and re-establish mission critical functions for less than catastrophic incidents.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

<p><b><u>AREA OF CONCERN:</u></b>  <i>EMERGENCY OPERATIONS</i></p>
<p><b><u>TOPIC:</u></b>  <i>EMERGENCY PREPAREDNESS</i></p>
<p><b><u>SUBTOPIC:</u></b>  <i>EMERGENCY PREPAREDNESS - PLANNING</i></p>
<p><b><u>EXPLANATION:</u></b>  This section describes the plans required to develop and maintain effective disaster preparedness/emergency management and business continuity programs.</p>
<p><b><u>INTENT:</u></b>  The survivability of critical infrastructures depends heavily on proper emergency preparedness planning that fully identifies threats and hazards, plans and executes mitigation measures, determines, directs and coordinates both internal and external response resources, and plans for and ensures the continuity of critical operations throughout an emergency event.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b>  An assessment of this area will include a review of emergency management programs and all plans, training and exercises related to emergency preparedness, response and continuity of operations.</p>
<p><b><u>BEST PRACTICES/INDUSTRY STANDARDS:</u></b>  Standards for the assessment of Emergency Operations were derived from the following:  Federal Emergency Management Agency (FEMA). Emergency management in the United States is by function and by law a cooperative effort on the part of all levels of government and the private sector. Within the Federal Government, FEMA serves as the lead agency for civil defense and coordinates with other federal agencies with responsibilities or capabilities valuable to national security emergency preparedness. Various FEMA publications and training courses are useful references.  Federal Emergency Management Agency (FEMA), "Guide for All-Hazard Emergency Operations Planning, State and Local Guide (101)"  The Federal Response Plan  Federal Regulations:  40 CFR 355 Emergency Planning and Community Right to Know Act  40 CFR 68 Risk Management Programs  29 CFR 1910.38 Employee Emergency Plans and Fire Prevention Plans</p>

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

PDD 67. Continuity of Operations

Federal Preparedness Circular (FPC) 65. Federal Executive Branch Continuity of Operations (COOP)

DoD Directive 3020.26, Continuity of Operations Policy and Planning

DoD Directive 3020.6. Assignment of National Security Emergency Preparedness Responsibilities to DoD Components

DoDI 6055.6. DoD Fire and Emergency Services Program

DoDI 2000.16. DoD Antiterrorism Standards  
DoDI 2000.18. DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines

UFC 3-600-01 Fire Protection for Facilities Engineering, Design and Construction.

Department of Transportation “ 2000 Emergency Response Handbook, A Guide for First Responders”

National Fire Protection Association (NFPA). The NFPA coordinates the development of various codes to promote and enhance fire prevention, life safety and emergency response. A number of NFPA codes directly pertain to emergency preparedness and response.

NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs.

Federal Preparedness Circular (FPC) 65. Federal Executive Branch Continuity of Operations (COOP)

DoD Directive 3020.6. Assignment of National Security Emergency Preparedness Responsibilities to DoD Components

DoDI 6055.6. DoD Fire and Emergency Services Program

DoDI 2000.16. DoD Antiterrorism Standards

DoDI 2000.18. DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines

UFC 3-600-01 Fire Protection for Facilities Engineering, Design and Construction.

Department of Transportation “ 2000 Emergency Response Handbook, A Guide for First Responders”

National Fire Protection Association (NFPA). The NFPA coordinates the development of various codes to promote and enhance fire prevention, life safety and emergency response. A number of NFPA codes directly pertain to emergency preparedness and response.

To meet mission assurance requirements for Emergency Preparedness Planning, the cognizant authority must address the following best practices:

1. Cognizant authority shall establish Disaster Preparedness/Emergency Management and Business Continuity Programs. The program shall include the following features:

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

- a. Program Management to include:
  - (1) Written program policy defining enabling authorities; vision and mission statements; goals, objectives, and milestones; management policies and procedures; program budget and management schedules.
  - (2) A Program Coordinator shall be designated and be authorized to administer and keep current the program in consultation with the Disaster Preparedness/Emergency Management Program Committee.
  - (3) A Program Committee shall be established and shall include at a minimum the Program Coordinator and others who have the appropriate expertise and knowledge of the entity and the authority to commit resources from all functional areas and shall solicit applicable external representation from relevant public and private entities.
  - (4) A capability to perform a comprehensive assessment of the program periodically to determine the overall effectiveness of the program.
- b. Threat and Hazard Identification and Vulnerability Assessment Processes
  - (1) Cognizant authority shall develop threat assessment and hazard identification processes that facilitate a genuine “all-hazards” approach to emergency planning.
- c. Threat and Hazard Mitigation Strategies
  - (1) Cognizant authority shall develop and implement interim and long-term threat and hazard mitigation strategies to eliminate or reduce the impact of identified threats and hazards.
- d. Resource Management
  - (1) Resource shortfalls should be identified and programmed for remediation.
  - (2) The need for mutual aid shall be determined and agreements established. Mutual aid agreements shall be referenced in appropriate program plans.
- e. Plans
  - (1) A family of plans shall be developed that include but are not limited to: Strategic Program Plan, Disaster Preparedness/Emergency Management Plan, Response Plans, Mitigation Plan, Recovery/Continuity of Operations Plan, Occupant Emergency Plan.
  - (2) The Strategic Plan shall define the vision, mission, goals, and objectives of the program as it relates to the policy of the entity.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

- (3) A Disaster Preparedness/Emergency Management Plan/Response Plan assigns responsibilities to organizations and individuals for carrying out specific actions at projected times and places in an emergency or disaster.
  - (4) The Mitigation Plan shall establish interim and long-term actions to eliminate threats and hazards or to reduce the impact of those hazards that cannot be eliminated.
  - (5) The Recovery/Continuity of Operations Plan shall identify the short-term and long-term priorities, processes, vital resources, acceptable time frames, and procedures for restoration of services, facilities, programs, and resources.
  - (6) The Occupant Emergency Plan defines employee responsibilities related to reporting emergencies, immediate damage control and fire fighting actions, facility evacuation procedures, public affairs and communications during an emergency incident.
- f. Direction, Control, and Coordination
- (1) Cognizant authority shall develop the capability to direct, control, and coordinate response and recovery operations.
  - (2) An incident management system shall be utilized and integrated with internal and external agencies.
  - (3) A mechanism shall be identified to determine the level of implementation of the incident management system according to the magnitude of the incident and the capability of the entity.
- g. Communications and Warning
- (1) Communications systems and procedures shall be established and regularly tested to support the program.
  - (2) Develop and maintain a reliable capability to alert public, officials, and emergency response personnel to get the desired actions implemented.
- h. Operations and Procedures
- (1) Cognizant authority shall develop, coordinate, and implement operational procedures to support the program. Update plans/procedures based on lessons learned from evaluation.
- i. Logistics and Facilities
- (1) A facility capable of supporting response and recovery operations shall be established, equipped, periodically tested, and maintained.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

- j. Training and Exercises
  - (1) Cognizant authority shall perform an assessment of training needs and shall develop and implement a training/education program to support the program.
  - (2) The objective of the training shall be to create awareness and enhance the skills required to develop, implement, maintain, and execute the program.
  - (3) Cognizant authority shall evaluate program plans, procedures, and capabilities through periodic exercises.
  - (4) Personnel shall be trained in the entity's incident management system.
  - (5) Procedures shall be established to ensure that corrective action is taken on any deficiency identified in the evaluation process and to revise the appropriate plan.
- k. Crisis Communications, Public Education, and Information
  - (1) Cognizant authority shall develop procedures to disseminate and respond to requests for pre-disaster, disaster, and post disaster information, including procedures to provide information to the media and deal with their inquiries.
  - (2) Implement a public education/awareness program to ensure standardized response actions.
- l. Finance and Administration
  - (1) Cognizant authority shall develop financial and administrative procedures to support the program before, during and following an emergency or disaster.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

<p><b><u>AREA OF CONCERN:</u></b> <i>EMERGENCY OPERATIONS</i></p>
<p><b><u>TOPIC:</u></b> <i>EMERGENCY RESPONSE</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>EMERGENCY RESPONSE - EXTERNAL</i></p>
<p><b><u>EXPLANATION:</u></b> External response refers to the availability and capability of non-organic emergency response organizations, generally limited to fire, rescue, and emergency medical services. Security specialists assess response by security forces.</p>
<p><b><u>INTENT:</u></b> To ensure cognizant authority has fully surveyed external emergency response resources and developed the plans and training necessary to ensure efficient response and effective coordination of first responders.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> An assessment of this area will include a survey of community emergency response resources, identification of relevant shortfalls in capability, and examine communications capabilities and procedures for coordinating external organizations.</p>
<p><b><u>BEST PRACTICES/INDUSTRY STANDARDS:</u></b> Standards for the assessment of Emergency Operations were derived from the following: Federal Emergency Management Agency (FEMA). Emergency management in the United States is by function and by law a cooperative effort on the part of all levels of government and the private sector. Within the Federal Government, FEMA serves as the lead agency for civil defense and coordinates with other federal agencies with responsibilities or capabilities valuable to national security emergency preparedness. Various FEMA publications and training courses are useful references. Federal Emergency Management Agency (FEMA), "Guide for All-Hazard Emergency Operations Planning, State and Local Guide (101)" The Federal Response Plan Federal Regulations:     40 CFR 355 Emergency Planning and Community Right to Know Act     40 CFR 68 Risk Management Programs     29 CFR 1910.38 Employee Emergency Plans and Fire Prevention Plans</p>

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

PDD 67. Continuity of Operations

Federal Preparedness Circular (FPC) 65. Federal Executive Branch Continuity of Operations (COOP)

DoD Directive 3020.6. Assignment of National Security Emergency Preparedness Responsibilities to DoD Components

DoDI 6055.6. DoD Fire and Emergency Services Program

DoDI 2000.16. DoD Antiterrorism Standards

DoDI 2000.18. DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines

UFC 3-600-01 Fire Protection for Facilities Engineering, Design and Construction.

Department of Transportation “ 2000 Emergency Response Handbook, A Guide for First Responders”

National Fire Protection Association (NFPA). The NFPA coordinates the development of various codes to promote and enhance fire prevention, life safety and emergency response. A number of NFPA codes directly pertain to emergency preparedness and response.

To meet mission assurance requirements for External Response, the cognizant authority must address the following best practices:

1. During a disaster or emergency incident, critical infrastructures depend on both organic and non-organic emergency response organizations to provide fire, rescue, HazMat, and emergency medical assistance. The continuity of critical functions and activities may depend on the responsiveness and capabilities of those organizations and on how well cognizant authority is able to coordinate their efforts.
2. Cognizant authority shall survey emergency response resources in their immediate communities. The survey should include organic resources, government emergency capabilities, private sector community resources, and higher-level government resources.
3. The survey shall identify capabilities and anticipated shortfalls. Experience indicates that shortfalls are likely to occur in personnel protective equipment and communications interoperability.
4. Cognizant authority shall factor capabilities of emergency response resources into Disaster Preparedness/Emergency Management Plans..
5. Cognizant authority shall establish a mechanism for coordinating various emergency response resources
6. Disaster Preparedness exercises should include external emergency response resources as participants whenever possible but at least often enough to ensure familiarity with the critical facilities.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

- |  |
|--|
| <ol style="list-style-type: none"><li>7. Cognizant authority shall address security and access issues so that first responders are not prevented from providing a timely and effective response.</li><li>8. Cognizant authority shall understand the incident command system utilized by local responders to assist in synchronized response and recovery.</li></ol> |
|--|

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

<p><b><u>AREA OF CONCERN:</u></b>  <i>EMERGENCY OPERATIONS</i></p>
<p><b><u>TOPIC:</u></b>  <i>EMERGENCY RESPONSE</i></p>
<p><b><u>SUBTOPIC:</u></b>  <i>EMERGENCY RESPONSE – INTERNAL</i></p>
<p><b><u>EXPLANATION:</u></b>  Internal response refers to those actions taken by personnel at the scene of an emergency incident when it occurs. These may include reporting, fire fighting or other damage control actions; actions to continue or transfer mission essential functions and services, shelter-in-place, and evacuation. Immediate response measures often limit or determine the ultimate severity of an emergency incident.</p>
<p><b><u>INTENT:</u></b>  To ensure cognizant authority has identified appropriate and desired immediate response actions, effectively communicated them to employees, and equipped and trained the employees to conduct the actions.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b>  An assessment of this area will review all plans, such as Occupant Emergency Plans, instructions, equipment and training related to internal, immediate response actions.</p>
<p><b><u>BEST PRACTICES/INDUSTRY STANDARDS:</u></b>  Standards for the assessment of Emergency Operations were derived from the following:  Federal Emergency Management Agency (FEMA). Emergency management in the United States is by function and by law a cooperative effort on the part of all levels of government and the private sector. Within the Federal Government, FEMA serves as the lead agency for civil defense and coordinates with other federal agencies with responsibilities or capabilities valuable to national security emergency preparedness. Various FEMA publications and training courses are useful references.  Federal Emergency Management Agency (FEMA), “Guide for All-Hazard Emergency Operations Planning, State and Local Guide (101)”  The Federal Response Plan  Federal Regulations:  40 CFR 355 Emergency Planning and Community Right to Know Act  40 CFR 68 Risk Management Programs  29 CFR 1910.38 Employee Emergency Plans and Fire Prevention Plans</p>

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

PDD 67. Continuity of Operations

Federal Preparedness Circular (FPC) 65. Federal Executive Branch Continuity of Operations (COOP)

DoD Directive 3020.6. Assignment of National Security Emergency Preparedness Responsibilities to DoD Components

DoDI 6055.6. DoD Fire and Emergency Services Program

DoDI 2000.16. DoD Antiterrorism Standards

DoDI 2000.18. DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines

UFC 3-600-01 Fire Protection for Facilities Engineering, Design and Construction.

Department of Transportation “ 2000 Emergency Response Handbook, A Guide for First Responders”

National Fire Protection Association (NFPA). The NFPA coordinates the development of various codes to promote and enhance fire prevention, life safety and emergency response. A number of NFPA codes directly pertain to emergency preparedness and response.

To meet mission assurance requirements for Internal Response, the cognizant authority must address the following best practices:

1. Cognizant authority should have plans, policies, and procedures in place that define immediate emergency response actions and assign responsibilities for carrying out those actions.
2. Immediate emergency response actions may be addressed in the Disaster Preparedness/Emergency Management Plan and more fully described in Occupant Emergency Plans.
3. Immediate emergency response actions are those that take place at the scene of an emergency incident or disaster prior to the arrival of external first responders and typically include incident reporting and notification, immediate fire fighting and other damage control actions, tasks required to continue or transfer essential functions and activities, and facility evacuation.
4. Cognizant authority should determine equipment required to support desired immediate emergency response actions and ensure that such equipment is installed, properly maintained, and periodically tested.
5. Cognizant authority shall ensure that employees are trained to carry out desired immediate emergency response actions.
6. Cognizant authority should conduct periodic exercises to test training and equipment. A system should be in place to ensure corrective actions are documented and implemented.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

7. Cognizant authority should possess the incident command and control structure, up and down the organization, to manage the incident from the time it is reported, through immediate actions, coordinating internal and external response, assessing damage, evaluating mission impact, and setting the stage for recovery.
8. An Emergency Response Team (ERT) should be designated and trained. The ERT is responsible for stabilizing an incident if possible or for gathering information and acting to support external First Responders if the incident requires external emergency response support. The ERT may be very small if the facility is limited in size and personnel and external emergency services resources are timely and adequate. A large facility or organization should organize a very capable team to better ensure asset survivability and mission continuity.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

**AREA OF CONCERN:**

*EMERGENCY OPERATIONS*

**TOPIC:**

*EMERGENCY PREPAREDNESS*

**SUBTOPIC:**

*EMERGENCY PREPAREDNESS - MITIGATION*

**EXPLANATION:**

Mitigation refers to efforts to eliminate or reduce the expected impact of identified threats and hazards that jeopardize personnel, property, or mission accomplishment. Mitigation efforts are generally accomplished prior to the emergency incident and include measures taken in the design and construction of facilities, fire detection and suppression systems, and measures that facilitate emergency response.

**INTENT:**

To ensure that all reasonable mitigation measures have been identified, prioritized, and implemented.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of this area will review facility design, hazard detection, monitoring, and response systems, notification and warning systems and procedures, and measures to more effectively identify and coordinate response capabilities. Significant emphasis is placed on fire detection and suppression because fire and associated smoke remains one of the most likely and most devastating potential hazards in any facility.

**BEST PRACTICES/INDUSTRY STANDARDS:**

Standards for the assessment of Emergency Operations were derived from the following:

Federal Emergency Management Agency (FEMA). Emergency management in the United States is by function and by law a cooperative effort on the part of all levels of government and the private sector. Within the Federal Government, FEMA serves as the lead agency for civil defense and coordinates with other federal agencies with responsibilities or capabilities valuable to national security emergency preparedness. Various FEMA publications and training courses are useful references.

Federal Emergency Management Agency (FEMA), "Guide for All-Hazard Emergency Operations Planning, State and Local Guide (101)"

The Federal Response Plan

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

Federal Regulations:

- 40 CFR 355 Emergency Planning and Community Right to Know Act
- 40 CFR 68 Risk Management Programs
- 29 CFR 1910.38 Employee Emergency Plans and Fire Prevention Plans

PDD 67. Continuity of Operations

Federal Preparedness Circular (FPC) 65. Federal Executive Branch Continuity of Operations (COOP)

DoD Directive 3020.6. Assignment of National Security Emergency Preparedness Responsibilities to DoD Components

DoDI 6055.6. DoD Fire and Emergency Services Program

DoDI 2000.16. DoD Antiterrorism Standards

DoDI 2000.18. DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines

UFC 3-600-01 Fire Protection for Facilities Engineering, Design and Construction.

Department of Transportation “ 2000 Emergency Response Handbook, A Guide for First Responders”

National Fire Protection Association (NFPA). The NFPA coordinates the development of various codes to promote and enhance fire prevention, life safety and emergency response. A number of NFPA codes directly pertain to emergency preparedness and response.

NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs.

To meet mission assurance requirements for Mitigation, the cognizant authority must address the following best practices:

1. Mitigation strategies shall be based on the results of threat and hazard identification, vulnerability assessments, program assessment, mission area analyses, operational experience, and overall risk assessments.
2. Mitigation strategies shall consider but not be limited to:
  - a. The use of appropriate building construction standards.
  - b. Hazard avoidance through appropriate land-use practices.
  - c. Relocation, retrofitting, or removal of structures at risk.
  - d. Removal or elimination of the hazard.
  - e. Reduction or elimination of the amount or size of the hazard.
  - f. Provision of protective systems or equipment.
  - g. Establishment of hazard warning and communications procedures.
  - h. Redundancy or duplication of critical systems, equipment, information, operations, or materials.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

- |   |
|---|
| <ul style="list-style-type: none"><li>i. The installation and maintenance of detection and suppression systems designed to protect mission essential functions, activities, and equipment. (Typically, fire protection engineers design systems that facilitate personnel evacuation and the survival of the overall structure without regard for critical functions and activities.)</li><li>j. Capabilities of emergency response organizations and the coordination necessary to ensure timely and effective emergency response.</li></ul> |
|---|

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

**AREA OF CONCERN:**

*EMERGENCY OPERATIONS*

**TOPIC:**

*EMERGENCY PREPAREDNESS*

**SUBTOPIC:**

*EMERGENCY PREPAREDNESS – THREAT AND HAZARD IDENTIFICATION*

**EXPLANATION:**

Threat and hazard identification is the first phase of emergency management and is essential to all other phases. In most cases it is not practical to prepare for every possible threat and hazard, as some will never occur. Therefore, it is essential that a full range of threats and hazards be identified, analyzed for probability, and assessed for likely impact. When possible both “worst case” and “most-likely case” scenarios should be developed so that hazard-specific response plans can be developed.

**INTENT:**

To ensure that cognizant authority has considered the full range of threats and hazards, has performed vulnerability analyses of both “worst case” and “most-likely case” scenarios and targeted response and continuity planning, procedures, equipment, and training accordingly.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of this area will include a review of the cognizant authority’s threat and hazard identification processes to ensure that a full range of threats and natural and technological hazards are considered and reasonable prioritized to facilitate efficient and effective emergency preparedness/response and mission continuity planning.

**BEST PRACTICES/INDUSTRY STANDARDS:**

Standards for the assessment of Emergency Operations were derived from the following:

Federal Emergency Management Agency (FEMA). Emergency management in the United States is by function and by law a cooperative effort on the part of all levels of government and the private sector. Within the Federal Government, FEMA serves as the lead agency for civil defense and coordinates with other federal agencies with responsibilities or capabilities valuable to national security emergency preparedness. Various FEMA publications and training courses are useful references.

Federal Emergency Management Agency (FEMA), “Guide for All-Hazard Emergency Operations Planning, State and Local Guide (101)”

The Federal Response Plan

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

Federal Regulations:

- 40 CFR 355 Emergency Planning and Community Right to Know Act
- 40 CFR 68 Risk Management Programs
- 29 CFR 1910.38 Employee Emergency Plans and Fire Prevention Plans

PDD 67. Continuity of Operations

Federal Preparedness Circular (FPC) 65. Federal Executive Branch Continuity of Operations (COOP)

DoD Directive 3020.6. Assignment of National Security Emergency Preparedness Responsibilities to DoD Components

DoDI 6055.6. DoD Fire and Emergency Services Program

DoDI 2000.16. DoD Antiterrorism Standards

DoDI 2000.18. DoD Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines

UFC 3-600-01 Fire Protection for Facilities Engineering, Design and Construction.

Department of Transportation “ 2000 Emergency Response Handbook, A Guide for First Responders”

National Fire Protection Association (NFPA). The NFPA coordinates the development of various codes to promote and enhance fire prevention, life safety and emergency response. A number of NFPA codes directly pertain to emergency preparedness and response.

NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs.

To meet mission assurance requirements for Threat and Hazard Identification, the cognizant authority must address the following best practices:

1. Effective emergency planning begins with a careful analysis of the full range of threats and hazards. Terrorist Threat Assessments should be part of the “all-hazards” approach to emergency planning.
2. Cognizant authority shall identify threats and hazards, the likelihood of their occurrence, and the vulnerability of people, property, critical infrastructures, missions, the environment, and the entity itself to those hazards. The hazards to be considered shall include, but not necessarily be limited to, natural hazards, technological hazards, human events to include criminal, enemy, subversive, and terrorist threats.
3. Cognizant authority shall conduct an impact analysis to determine the potential for detrimental impacts of the hazards on items including but not limited to the following:
  - a. The entity’s essential functions and activities.
  - b. Health and safety of personnel in the area at the time of the incident.
  - c. Health and safety of personnel responding to the incident.

**For Official Use Only**  
**DTRA-Recommended Emergency Operations Standards**

- |  |
|--|
| <ul style="list-style-type: none"><li>d. Continuity of Operations.</li><li>e. Property, facilities, and infrastructure.</li><li>f. The environment.</li><li>g. Regulatory and contractual obligations.</li></ul> <p>4. Cognizant authority shall develop and implement a strategy to eliminate threats and hazards or mitigate the effects of hazards that cannot be eliminated.</p> |
|--|

**For Official Use Only**  
**DTRA-Recommended Structural Response Standards**

**DTRA-RECOMMENDED STRUCTURAL RESPONSE**

<p><b><u>AREA OF CONCERN:</u></b> <i>STRUCTURAL RESPONSE</i></p>
<p><b><u>TOPIC:</u></b> <i>CRITICAL EQUIPMENT/COMPONENT DAMAGE</i></p>
<p><b><u>SUBTOPIC:</u></b> <i>PROTECTION</i></p>
<p><b><u>EXPLANATION:</u></b> Mission critical equipment, and the associated support systems, must function properly to ensure mission continuity. Thus, facilities must consider not only survivability of structures, but also protection of equipment housed in these facilities.</p>
<p><b><u>INTENT:</u></b> The intent of this process is to ensure adequate protection of critical equipment against the effects of explosives. Survival of the structure is important for equipment survival, but facility survival does not ensure equipment survival. Equipment fragility must be assessed, and compared against the expected explosive environment.</p>
<p><b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> To assess equipment damage from the design blast threats(s), consideration shall be given to the factors that affect structural survival (such as standoff, adequacy of barriers and protective procedures, etc). If the facility appears to survive, then additional analysis shall be performed to evaluate the environment imposed on critical equipment. The environment may include air blast overpressure, ground shock, primary fragments, and/or secondary fragments. Position of critical equipment relative to vulnerable exterior wall or windows and the existence or absence of isolation and shock mounting are important additional considerations.</p>
<p><b><u>BEST PRACTICES/INDUSTRY STANDARDS:</u></b></p> <ol style="list-style-type: none"><li>1. Generally, standards do not exist for protection of equipment against blast effects. Specific classes of equipment should be evaluated separately from each other.</li><li>2. The Shock and Vibration Information Analysis Center has the best available compilation of equipment fragility information in its "<i>Component Vulnerability Analysis Archive.</i>"</li></ol>

**For Official Use Only**  
**DTRA-Recommended Structural Response Standards**

3. Computational and blast code methods described in the *Army Technical Manual Design and Analysis of Hardened Structures to Conventional Weapons Effects (TM 5-855-1, dated August 1998)* and its associated family of blast codes called *Protective Structures Automated Design System (PSADS)*, available from the Defense Threat Reduction Agency (DTRA) are also useful.
4. Other references with tables and descriptions of the blast resistance of various types of equipment include *Army Technical Manual (TM) Structures to Resist the Effects of Accidental Explosions (TM 5-1300, dated November 1990)* and *Army TM Explosive Ordnance Disposal Procedures (TM 60A-1-1-4, dated 11 April 1998)*.

**For Official Use Only**  
**DTRA-Recommended Structural Response Standards**

**AREA OF CONCERN:**

*STRUCTURAL RESPONSE*

**TOPIC:**

*NEW CONSTRUCTION OR RENOVATION*

**SUBTOPIC:**

*PROTECTIVE DESIGN*

**EXPLANATION:**

Construction standards/specifications incorporated into the design and construction of new structures or renovation of existing structures impact significantly on the facility's overall survivability against attack. For critical facilities, mission survival after an attack is often essential to the national defense.

**INTENT:**

The intent is to ensure adequate protection for critical facilities from terrorist attack through an understanding of the potential damage associated with a selected level of protection.

**DESCRIPTION OF AREAS TO BE ASSESSED:**

An assessment of the adequacy of critical facility design and construction shall consider: the facility's design basis threat(s); the current range of threats identified for the assessment; desired level of protection against each threat; basis for design and selection of structural building components; and predicted damage from design threats. The assessment will compare predicted damage against the description of damage associated with the facility's desired level of protection to ensure the desired level of protection will be met. If not, incorporate construction specifications and measures achieving greater resistance to attack.

**BEST PRACTICES/INDUSTRY STANDARDS:**

The *United Facilities Criteria (UFC) DoD Minimum Antiterrorism Standards for Buildings (UFC 4-010-01, dated 8 October 2003)* describes minimum construction standards required of new and existing DoD facilities. The UFC standards also define the levels of protection and associated damage for comparison against assessed damage caused by design threats.

*USA TM 5-853, Vol 1/2/3/4 Security Engineering Manual (Oct 1994)* provides a process for determining appropriate security enhancements during facility design to achieve selected levels of protection against various anticipated levels of threat.

1. Design specifications and plans for new construction and major renovation of existing structures should incorporate all applicable DoD minimum antiterrorism (AT) construction standards.

**For Official Use Only**  
**DTRA-Recommended Structural Response Standards**

2. Design basis threats particularly for older structures and structures not originally intended to house critical functions are generally inadequate for achieving the desired level of protection in current threat environments. DoD recognized blast damage codes such as AT Planner, BEEM, WinDAS, WinGARD, HazL, CONWEP, FACEDAP, WAC, and PSADS shall be used to predict damage of critical facilities against the full range of threats identified for the vulnerability assessment. Accurate damage prediction may require comparison and analysis of results from several codes, with understanding of the strengths and limitations of each code.
3. If no blast damage codes are available, table-based references may be used to predict structural damage/injuries. Applicable references include: the BELT tables; Army Engineer Technical Letter (ETL) *Estimating Damage to Structures from Terrorist Bombs Field Operations Guide* (ETL 1110-3-49, dated 14 July 1999); Navy User's Guide (UG) *User's Guide on Protection Against Terrorist Vehicle Bombs* (UG 2031-SHR, dated December 1998); Army Technical Manual (TM) *Structures to Resist the Effects of Accidental Explosions* (TM 5-1300, dated November 1990), and Army TM *Security Engineering* (TM 5-853-1/2/3/4, dated May 1994). To ensure mission survival following an attack, the facility should accept damage no greater than "low" or "minor."
4. Critical facilities should be augmented with several layers of security including exclusive perimeters and less exclusive outer perimeters each with its own access control capabilities and procedures. Consideration shall be given to the total security system when analyzing the adequacy of facility construction and design. Iterative analyses may be required to determine the most cost-effective mix of security system components that will best contribute to asset survival and mission continuity.

**For Official Use Only**  
**DTRA-Recommended Threat Standards**

**DTRA-RECOMMENDED THREAT**

<b><u>AREA OF CONCERN:</u></b> <i>THREAT</i>
<b><u>TOPIC:</u></b> <i>ELECTROMAGNETIC THREATS</i>
<b><u>SUBTOPIC:</u></b> <i>RF WEAPONS, EMP, GROUNDING, BONDING, LIGHTNING PROTECTION</i>
<b><u>EXPLANATION:</u></b> EMP/EMI/EMC/URE/RF Threats
<b><u>INTENT:</u></b> Perform a comprehensive assessment of EMP/EMI/EMC/URE/RF Threats to Customer's mission in the context of all other mission operations.
<b><u>DESCRIPTION OF AREAS TO BE ASSESSED:</u></b> Mission operations can be disrupted or halted indefinitely due to interruption and /or damage of critical mission-specific electrical system components. Damage mechanisms can include weapons, collateral effects of weapons, and natural hazards.
<b><u>BEST PRACTICES/INDUSTRY STANDARDS:</u></b> <ol style="list-style-type: none"><li>1. MILSTD-188-125, Vol I and II, for general EMP protection</li><li>2. MILSTD-2169B, EMP threat waveform specifications</li><li>3. National Fire Prevention Association (NFPA) 780, industrial standard for lightning protection systems</li><li>4. MIL-HDBK-1004/6 on lightning protection</li><li>5. U.S. Air Force Instruction (AFI) 32-1065, on grounding and bonding</li><li>6. U.S. Air Force Manual (AFMAN) 91-201, OP-04, OP-05, and OP-3565, on explosives safety</li><li>7. MIL-HDBK-419A and modifications, on grounding, bonding, and shielding for electronic equipment and facilities</li><li>8. TM 5-690 and modifications, grounding, bonding, and shielding for C4ISR facilities</li><li>9. MIL-STD-464 and modifications, electromagnetic environmental effects requirements for systems</li><li>10. MIL-HDBK-1857, DoD handbook on grounding, bonding, and shielding practices</li></ol>

**For Official Use Only**  
**Draft CIP FSVA – Acronym List**

**ACRONYM LIST**

<b>Acronym</b>	<b>Description</b>
AF	Architecture Framework
AFR	Air Force Regulation
AIS	Automated Information System
AM	Alarm Monitors
AOC	Army Operations Center
AOR	Areas of Responsibility
APHIS	Animal Plant Health Inspection Service
AR	Acceleration Request
AS	Area Supervisor
AT	Antiterrorism
ATO	Antiterrorism Officer
ATS	Automatic Transfer Switches
AT/FP	Antiterrorism/Force Protection
BF	Backup Force
BS	Boundary Sentries
BSC	Biosafety Cabinetry
BSL	Biosafety Level
CA	Commercial Activities
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CCTV	Closed Circuit Television
CDC	Centers for Disease Control
CDPR	Chemical Duty Position Roster
CERT/CC	Communication with Computer Emergency Response Team/Command Center
CFR	Conceptual Functional Requirements
CIP	Critical Infrastructure Program
CMA	Competent Medical Authority
COCO	Contractor Owned, Contractor Operated
CONUS	Continental United States

**For Official Use Only**  
**Draft CIP FSVA – Acronym List**

Acronym	Description
COOP	Continuity of Operations Plans
COR	Contracting Officers Representative
COTS	Commercial off-the shelf
CPU	Central Processing Unit
CSA	Cognizant Security Agency
DCID	Director of Central Intelligence Directive
DNS	Domain Naming Service
DoD	Department of Defense
DoDD	DoD Directive
DoDI	Department of Defense Infrastructure
DOJ	Department of Justice
DTRA	Defense Threat Reduction Agency
EC	Entry Controllers
ECR	Entry Control Roster
EED	Electro-Explosive Devices
EEFI	Essential Elements Friendly Information
EMS	Emergency Medical Services
EO	Executive Order
EOD	Explosive Ordinance Disposal
ERP	Emergency Response Plan
ERT	Emergency Response Team
ESS	Electronic Security Systems
FCL	Facility Clearances
FEDCERT/CC	Federal Computer Emergency Response Team/Command Center
FISCAM	Federal Information System Controls Manual
FPC	Federal Preparedness Circular
FPCON	Force Protection Condition
FSO	Facility Security Officers
GCA	General Contracting Agency
GOCO	Government Owned, Contractor Operated
GSA	General Services Administration

**For Official Use Only**  
**Draft CIP FSVA – Acronym List**

Acronym	Description
HAZMAT	Hazardous Materials
HHS	Health and Human Services
HPA	High Priority Agents and Toxins
HQDA	Headquarters, Department of Army
HVAC	Heating, Ventilation, Air Conditioning
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
ID	Identification
IDS	Intrusion Detection Systems
IED	Improvised Explosive Device
IRF	Incident Response Force
IRM	Information Resources Management
IT	Information Technology
JSIVA	Joint Staff Integrated Vulnerability Assessment
JTS	Joint Tactical Simulation
LAA	Limited Access Authorizations
LEPC	Local Emergency Planning Committees
MACOM	Major Command (USA)
MAJCOM	Major Command (USAF)
MILCON	Military Construction
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	National Agency Check
NFPA	National Fire Protection Association
NIH	National Institutes of Health
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCONUS	Outside Continental United States
ODCSOPS (G-3)	Office of the Deputy Chief of Staff for Operations (Army)

**For Official Use Only**  
**Draft CIP FSVA – Acronym List**

Acronym	Description
OJT	On-the-job Training
OMB	Office of Management and Budget
OPNAVINST	Operation Navy Instruction
OPSEC	Operational Security
OSHA	Occupational Safety & Health Act
PBX	Private Branch Exchange
PCL	Personnel Clearances
PPF	Pre-designated Firing Position
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPE	Personnel Protective Equipment
PRP	Personnel Reliability Program
PSI	Personal Security Investigation
RAC	Risk Assessment Code
RAM	Reliability, Availability and Maintainability
RCWM	Recovered Chemical Warfare Material
RDT&E	Research, Development, Test and Evaluation
RF	Radio Frequency
ROE	Rules of Engagement
SAN	Separately Accredited Network
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facilities
SDD	Standard Design Drawing
SES	Senior Executive Service
SME	Subject Matter Expert
SOP	Standard Operating Procedures
SRT	Special Response Teams
SSN	Social Security Number
SSS	Security Support Structure
TEU	Technical Escort Unit
UFC	Unified Facility Criteria

**For Official Use Only**  
**Draft CIP FSVA - Acronym List**

<b>Acronym</b>	<b>Description</b>
UL	Underwriters Laboratory
UPS	Uninterruptible Power Supply
US	United States
USACE	U.S. Army Corps of Engineers
USACIDC	U.S. Army Center for Infectious Disease Control
USASC	The U.S. Army Safety Center
USDA	U.S. Department of Agriculture
VA	Department of Veterans Affairs
VIP	Very Important Person
WSV	Weapons Storage Vault
WS3	Storage and Security System