

Department of Defense Full Spectrum Integrated Vulnerability Assessment Program

Critical Infrastructure Protection Vulnerability Assessment Capability Area Concept of Operations



1 March 2004

For Official Use Only
DRAFT



**The Defense Program Office for
Mission Assurance**

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

**Draft
Critical Infrastructure Protection Capability Area
Concept of Operations**

March 2004

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

**DRAFT
For Official Use Only**

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

CONTENTS

<u>Section</u>		<u>Page</u>
ES	EXECUTIVE SUMMARY	ES-1
1.0	INTRODUCTION	1
1.1	Purpose	1
1.2	Background	1
1.3	Scope	2
1.4	Intended Audience	2
1.5	References	2
2.0	OPERATIONAL CONCEPT	3
2.1	Critical Asset Nomination and Prioritization Criteria	3
2.2	CIP Capability Area Assessment Methodology	4
2.3	CIP Capability Area Standards and Requirements	4
2.3.1	CIP Capability Area Standards.....	4
2.3.2	CIP Capability Area Output Requirements.....	6
2.3.3	FSIVA CIP Capability Area Technical Report Requirements	6
2.3.4	FSIVA CIP Capability Area Data Element Requirements	6
2.3.5	After-Action Report Requirements.....	7
2.4	FSIVA Vulnerability Tracking Process	7
3.0	ROLES AND RESPONSIBILITIES.....	7
3.1	Assistant Secretary of Defense for Homeland Defense (ASD[HD]).....	7
3.2	Joint Staff Deputy Director for Anti-Terrorism/Homeland Defense (DDAT/HD)	8
3.3	Defense Program Office for Mission Assurance (DPO-MA).....	8
3.4	Combatant Commanders.....	9
3.5	Military Departments	9
3.6	DoD Lead Component Agencies	9
3.7	DoD FSIVA Program Assessment Organizations.....	9
4.0	EDUCATION AND TRAINING	10
5.0	CONCLUSION.....	10

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

CONTENTS (CONTINUED)

<u>Appendix</u>	<u>Page</u>
A	CRITICAL ASSET NOMINATION AND PRIORITIZATION CRITERIA A-1
B	ASSESSMENT METHODOLOGY FOR THE CIP CAPABILITY AREA.....B-1
B.1	FSIVA Team GuidanceB-2
B.1.1	Team CompositionB-2
B.1.2	Team Member TrainingB-2
B.1.3	Procedures for Handling Critical Infrastructure InformationB-2
B.2	Steps in the FSIVA processB-2
B.2.1	FSIVA TaskingB-2
B.2.2	Pre-assessment Requirements and Processes.....B-3
B.2.3	Team Advance PreparationB-3
B.2.4	Team Final PreparationB-4
B.2.5	Team Pre-Assessment Visit.....B-4
B.2.6	On-site Assessment Requirements and ProcessesB-5
B.2.6.1	Conduct On-Site AssessmentB-5
B.2.6.2	Verify Impact of Asset Loss or Disruption.....B-5
B.2.6.3	Assess ThreatB-5
B.2.6.4	Assess Vulnerabilities.....B-6
B.2.6.5	Assess RiskB-7
B.2.6.6	Analyze CountermeasuresB-7
B.2.6.7	Develop Initial Out-brief (On-site)B-8
B.2.6.8	Prepare Final ReportsB-8
B.2.6.9	Issue Final Report (Within 30 days of Assessment).....B-9
B.2.7	CIP Capability Area Follow-up Assessment Requirements and ProcessesB-9
C	FSIVA STANDARDS FOR THE CIP CAPABILITY AREA C-1
C.1	Physical Security C-3
C.2	Information Security C-3
C.3	Personnel Security..... C-3
C.4	Industrial Security..... C-3
C.5	Safety..... C-4
C.6	Plans..... C-4
C.7	Operational Security (OPSEC) C-4
C.8	Nuclear Security C-4
C.9	Chemical Security C-4

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

CONTENTS (CONTINUED)

<u>Appendix</u>	<u>Page</u>
C.10 Biological Security.....	C-4
C.11 Supporting Infrastructure Networks	C-5
C.12 Commercial Relationships.....	C-5
C.13 Threats	C-5
C.14 Countermeasure Recommendations.....	C-5
C.15 Weapons of Mass Destruction.....	C-Error! Bookmark not defined.
C.16 Structural Response	C-Error! Bookmark not defined.
C.17 Emergency Operations.....	C-Error! Bookmark not defined.
D REPORTING REQUIREMENTS FOR THE CIP CAPABILITY AREA.....	D-1
D.1 Report Content/Organization for the FSIVA CIP Capability Area (Web-based System)	D-2
D.2 Executive Summary	D-2
D.2.1 Asset Identification.....	D-2
D.2.2 Security Classification.....	D-3
D.2.3 Objectives of the FSIVA	D-3
D.2.4 Organization of the Assessment Team.....	D-3
D.2.5 Modules Assessed	D-3
D.2.6 Conclusions	D-3
D.2.7 Noteworthy Items.....	D-3
D.2.8 Items for Further Action.....	D-3
D.3 Body of the Report.....	D-4
D.3.1 Introduction.....	D-4
D.3.2 Site Description	D-4
D.3.3 Asset Owner Furnished Information.....	D-5
D.3.4 Records Review.....	D-5
D.3.5 Site Assessment.....	D-5
D.3.6 Interviews	D-5
D.3.7 Findings.....	D-6
D.3.8 Impact.....	D-6
D.3.9 Conclusions	D-6
D.3.10 Recommendations	D-6
D.3.11 Deviations	D-6
D.3.12 Additional Services	D-6
D.3.13 References	D-7

**For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations**

CONTENTS (CONTINUED)

<u>Appendix</u>	<u>Page</u>
D.3.14 Qualifications for the Team.....	D-7
D.3.15 Appendices.....	D-7
E DATA ELEMENT REQUIREMENTS FOR THE CIP CAPABILITY AREA	E-1
F AFTER-ACTION REPORT REQUIREMENTS	F-1
G TRACKING PROCESS FOR THE CIP CAPABILITY AREA.....	G-1

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

EXECUTIVE SUMMARY

The intent of this document is to address the need for a defense-wide, comprehensive, fully integrated, and sustainable vulnerability assessment process to ensure protection and availability of defense, national, and international assets critical to our National Security in peace, crisis, and war.

Based on the direction of the Office of the Assistant Secretary of Defense for Homeland Defense (OASD(HD)), the Defense Program Office for Mission Assurance (DPO-MA) has developed the Department of Defense (DoD) Full Spectrum Integrated Vulnerability Assessment (FSIVA) Program. The FSIVA Program defines the process within DoD for conducting vulnerability assessments in the capability areas of Anti-Terrorism/Force Protection (AT/FP), Critical Infrastructure Protection (CIP) and Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE). This objective is being achieved by examining appropriate information on vulnerability assessment activities within the DoD, synthesizing best practices to create an all-inclusive vulnerability assessment process, and developing applicable standards of practice for the DoD FSIVA.

The FSIVA CIP capability area will comprehensively, uniformly, and consistently evaluate the vulnerabilities of critical physical and cyber assets that are essential to mobilize, deploy, and sustain United States (U.S.) military operations. The FSIVA will address the full range of areas with which CIP is concerned.

The DPO-MA has outlined program objectives and requirements necessary to accomplish the goals of the CIP capability area. This capability area will consist of standards for the conduct of the CIP portion of the FSIVA, the development and management of a database capable of supporting the recording and archiving of asset vulnerability data, and a tracking mechanism designed to capture all applicable reported vulnerabilities and associated remediation efforts. Additionally, the program will ensure that all DoD CIP vulnerability assessments are conducted in a consistent manner by FSIVA-trained organizations. The DPO-MA will develop a FSIVA training program that will be made available to all participating vulnerability assessment organizations.

An integrated vulnerability assessment program will enable DoD to achieve accurate data; conduct appropriate analysis; and provide Combatant Commanders, Services, Agencies, and Sectors access to assessment information on vulnerabilities that could potentially impact their ability to conduct successful operations.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

1.0 INTRODUCTION

1.1 PURPOSE

The Department of Defense (DoD) has long understood the need to develop, implement and sustain a vulnerability assessment program that will comprehensively and consistently assess vulnerabilities of DoD critical assets. To satisfy this need, the Defense Program Office for Mission Assurance (DPO-MA) has been tasked by the Office of the Assistant Secretary of Defense for Homeland Defense (OASD[HD]) to establish and implement the DoD Full Spectrum Integrated Vulnerability Assessment (FSIVA) Program. This program will address FSIVA requirements, standards and protocols within the Anti-Terrorism/Force Protection (AT/FP), Critical Infrastructure Protection (CIP) and Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) capability areas.

The concepts within this document focus on the FSIVA CIP capability area. The intent of this document is to address the need for a defense-wide, comprehensive, fully integrated, repeatable and sustainable vulnerability assessment process to ensure protection and availability of defense, national, and international assets critical to our National Security in peace, crisis, and war.

1.2 BACKGROUND

The mission of the DoD CIP Program is to protect against the loss or degradation of critical assets that affect the warfighting capability of United States (U.S.) armed forces and, ultimately, our national defense and economic security. It is DoD policy that there be an integrated mission assurance program to identify, analyze, and assess DoD assets, non-DoD assets, and infrastructure critical to DoD force projection and sustainment; to provide for their protection and assurance; and to train and equip personnel to analyze, assess, protect, remediate, and restore these assets.

Vulnerability Assessments are an integral part of mission assurance, yet there exists no defense-wide, comprehensive, fully integrated, repeatable, and sustainable vulnerability assessment process to ensure protection and availability of assets critical to National Security. While there are numerous organizations within DoD that perform vulnerability assessments, each of these organizations has independently produced assessment standards. The establishment of universal assessment requirements and standards is necessary to achieve an integrated, capabilities-based vulnerability assessment program.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

To satisfy this need, the DPO-MA has initiated the development of the DoD FSIVA Program.

1.3 SCOPE

The Concept of Operations focuses on the CIP capability area of the overarching FSIVA Program. The CIP capability area consists of modules developed to sufficiently address the full range of areas with which CIP is concerned. The FSIVA CIP capability area will be operational in FY05.

1.4 INTENDED AUDIENCE

The intended audience for the Concept of Operations includes the ASD (HD) CIP Directorate in its policymaking role, the Joint Staff Deputy Director for Global Operations Anti-Terrorism and Force Protection (DDGO-AT/FP) for its policy making role and responsibility for program integration among the Combatant Commands and Services, the DPO-MA , for its role in the establishment and implementation of the program, and the CIP community as a whole in its collective role in assisting in development of the program and in the conduct of DoD FSIVA's.

1.5 REFERENCES

- a. Department of Defense Instruction 3020, Implementation of the Critical Infrastructure Protection Program (in coordination)
- b. The Department Of Defense Critical Infrastructure Protection (CIP) Plan, 18 November 1998
- c. Department of Defense Critical Infrastructure Protection Strategy, April 2003
- d. Department of Defense Critical Infrastructure Protection (CIP) Analysis and Assessment Process Summary
- e. Analysis and Assessment Strategy for the CIP Documentation Hierarchy, March 2003
- f. A Total Risk-based Management Methodology for Critical Infrastructure Protection, November 2002 (draft)

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

- g. Critical Infrastructure Protection Database Architecture Description and Needs, 17 March 2003 (draft)

Below references may be relocated at later date:

- a. DPO-MA CIP Program CONOPS (in development)
- b. DPO-MA DoD Full Spectrum Integrated Vulnerability Assessment Program CONOPS (in development)
- c. DPO-MA CIP Enterprise Architecture Strategy Document (in development)

2.0 OPERATIONAL CONCEPT

The FSIVA CIP capability area will comprehensively, uniformly, and consistently evaluate the vulnerabilities of critical physical and cyber assets that are essential to mobilize, deploy, and sustain U.S. military operations. This portion of the FSIVA will address the full range of areas with which CIP is concerned. Specifications for a set of consistent outputs from FSIVAs will enable DoD to archive data, conduct appropriate analysis, and reliably share information with all DoD components involved in mission assurance. Critical assets that will be assessed may include those of DoD, U.S. commercial/private sector, foreign commercial/private sector, and host nations.

2.1 CRITICAL ASSET NOMINATION AND PRIORITIZATION CRITERIA

The first step in the FSIVA CIP capability area process is the nomination and prioritization of critical assets. The process for nominating and prioritizing critical assets for the purpose of conducting a FSIVA within the CIP capability area implies a process by which assets may be differentiated and rank-ordered for assessment. The DPO-MA is currently working to develop a prioritization process with associated nomination criteria that is intended to meet the overarching needs of the DoD by focusing on the identified priorities stated in the National Military Strategy (NMS). Critical Asset Nomination Criteria and a prioritization concept are located in Appendix A of this document.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

2.2 CIP CAPABILITY AREA ASSESSMENT METHODOLOGY

CIP capability area assessment methodology is currently under development.

The DPO-MA has developed a draft methodology for the conduct of the FSIVA CIP capability area. This methodology includes FSIVA team member guidance, tasking and preparation processes and requirements, pre-assessment processes and requirements, on-site assessment processes, analysis requirements and methodologies, and follow-on assessment processes and requirements to be adhered to by the FSIVA assessor. An outline of the step-by-step process with key bullets of each step in the approach and descriptive text summaries to provide a detailed explanation of the envisioned approach are located in Appendix B.

2.3 CIP CAPABILITY AREA STANDARDS AND REQUIREMENTS

The DPO-MA will develop the necessary policies and processes to ensure there is an effective and integrated approach to assessing the vulnerabilities of identified critical assets. To that end, a comprehensive, consistent, and repeatable vulnerability assessment process that incorporates uniform assessment requirements and standards will be established. The DPO-MA has developed an initial set of Output Requirements and Assessment Standards for the CIP capability area.

2.3.1 CIP Capability Area Standards

The purpose of the FSIVA standards for the CIP capability area is two-fold. First, the standards will prescribe the areas that will be assessed during the conduct of FSIVAs on DoD designated critical assets. Second, the standards will guide the assessor in evaluating and identifying vulnerabilities associated with those designated critical assets.

The overall assessment 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 assets designated as critical by the DoD. 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.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

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 comprehensive and appropriately detailed to identify all critical asset vulnerabilities.

These standards are applicable to all DoD critical assets, to include non-DoD Federally-owned or leased critical assets, and commercial critical assets that support a specified DoD mission.

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 standards. This foundation established a basis for the standards, rooted in already accepted vulnerability assessment performance standards and guidelines. The adapted CIP capability area standards were then tailored, as required, to ensure their applicability to the broadest possible range of potential critical assets. The standards 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 an assessment in the CIP capability area. The standards are intended for use by both the designated FSIVA assessors and the critical asset owners. In general, these standards will be used to:

a. Establish the overarching baseline set of assessment standards for critical assets to assist in the protection of these identified and validated critical assets.

b. Establish the different areas of concern and associated standards a FSIVA within the CIP capability area will examine during an assessment.

c. Assist in the training of FSIVA assessors.

An outline of the areas of concern contained within the CIP capability area standards can be found in Appendix C.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

2.3.2 CIP Capability Area Output Requirements

Output Requirements are those requirements DoD FSIVA assessors must accomplish to satisfy the FSIVA Program reporting requirements. CIP capability area Output Requirements include Reporting Requirements, Data Element Requirements, and After-Action Report Requirements and are outlined in greater detail in Appendices D, E, and F, respectively.

2.3.3 FSIVA CIP Capability Area Technical Report Requirements

The CIP capability area will help to achieve the DoD CIP objective of providing senior DoD leadership and Combatant Commanders with quantifiable measures of mission-essential critical asset vulnerabilities. The data gathered during the assessment will support the identification of risks to military capabilities and operations, and assist in deliberate and crisis-action planning processes. To develop a comprehensive and consistent FSIVA CIP capability area Technical Report, it is necessary that critical asset data collected be consistent. This consistency will facilitate the accomplishment of CIP capability area objectives and accommodate mission assurance planning.

In all FSIVAs, a final vulnerability assessment report must be provided. The final report will outline the data collected by the assessment team as it supports the findings and conclusions of the assessment. This report will be used to inform and notify management of their critical asset vulnerabilities; will assist in the initiation of remediation actions; and will be the basis for tracking of the critical asset, its vulnerabilities, and remediation actions taken. Specific report requirements for the CIP capability area are outlined in Appendix D.

2.3.4 FSIVA CIP Capability Area Data Element Requirements

Organizations conducting assessments within the CIP capability area must provide assessment data to the DPO-MA for incorporation to the CIP Database. The CIP Database is a mission assurance tool that addresses each of the DoD CIP activities. This tool will provide DoD senior leaders and Combatant Commanders with critical information that will assist them in making risk-management decisions. The data from the CIP capability area must be incorporated into the DoD CIP Database to ensure that Combatant Commands, Services, Agencies, and Sectors have access to assessment information on critical asset vulnerabilities that could impact their ability to conduct peacetime, crisis, and wartime operations. The draft data elements the assessor is required to provide to the DPO-MA for incorporation into the CIP Database are outlined in Appendix E of this document.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

2.3.5 After-Action Report Requirements

Organizations conducting FSIVAs must provide an After-Action Report to the DPO-MA. This After-Action Report will be utilized for Program Management purposes and will require the assessment organization to report on all aspects of the process, including recommendations for changes to future assessments. Minimum elements of the FSIVA After-Action Report for the CIP capability area are outlined in Appendix F of this document.

2.4 FSIVA VULNERABILITY TRACKING PROCESS

The FSIVA Vulnerability Tracking Process is currently under development.

The DPO-MA has developed a draft concept for tracking FSIVA Program assessments, including results, countermeasure recommendations and associated costs, remediation efforts, and follow-on assessments.

A comprehensive FSIVA tracking tool is intended to support several processes and serve as a source of meaningful information on several levels. First, the FSIVA tracking tool is intended to assist the DPO-MA in the coordination and scheduling process of the FSIVAs, including follow-up visits to ensure that the countermeasures that were installed did not inadvertently introduce new vulnerabilities. Second, the tracking instrument is intended to provide an official record of all FSIVAs conducted, the results (to include all identified vulnerabilities), and subsequent countermeasures that are implemented as part of remediation efforts. Third, this tracking tool is intended to provide a basis of support for the planning, programming, budgeting, and execution (PPBE) submissions for funding of remediation efforts. Finally, this tool will assist senior managers in aggregating information that depicts the benefits, measured in risk reduction over time, derived from the expenditure of targeted remediation funding. Draft examples of the types of data fields that would support these respective functions are outlined in Appendix G of this document.

3.0 ROLES AND RESPONSIBILITIES

3.1 THE ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE (ASD[HD])

The Assistant Secretary of Defense for Homeland Defense (ASD[HD]) shall act as the principal staff assistant and advisor on the DoD CIP FSIVA Program, and provide

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

FSIVA policy oversight and ensure compliance with applicable DoD Directives by all Department of Defense components.

3.2 THE JOINT STAFF DEPUTY DIRECTOR FOR GLOBAL OPERATIONS ANTI-TERRORISM/FORCE PROTECTION (DDGO-AT/FP)

The role of the Joint Staff DDGO(J34) is to provide oversight and coordination of the FSIVA Program among combatant commands and services in order to facilitate FSIVA planning and the translation of policy into action.

3.3 THE DEFENSE PROGRAM OFFICE FOR MISSION ASSURANCE (DPO-MA)

The FSIVA Program will be managed by the DPO-MA. The DPO-MA will be responsible for the development and oversight of all program initiatives. In support of this management responsibility, DPO-MA has established FSIVA Program Coordinator billets. The FSIVA Program Coordinators are responsible for the coordination, planning, scheduling, and budgeting related to the development of the program. The specific responsibilities of the FSIVA Program Coordinators include, but are not limited to the following:

a. The DPO-MA shall support the development of DoD FSIVA policy and ensure it is clear, comprehensive, and followed by all DoD assessment organizations. This policy will include providing input to the development of a DoD FSIVA Directive, Instruction, and any other required policy documentation.

b. The DPO-MA shall develop and maintain the DoD FSIVA Program Management Plan to ensure updates and changes to the program are properly recorded.

c. The DPO-MA shall develop DoD FSIVA requirements, assessment standards, protocol, and associated assessment methodology that must be properly socialized with the DoD vulnerability assessment community.

d. The DPO-MA shall develop a FSIVA Training Program and associated User's Guide to ensure all DoD assessors are adequately prepared to conduct consistent, repeatable, and comprehensive vulnerability assessments.

e. The DPO-MA is responsible for all coordination and tasking of FSIVAs.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

f. The DPO-MA shall develop, implement and manage a database capable of supporting the recording and archiving of asset vulnerability data, tracking, remediation progress, and sharing vulnerability assessment lessons learned. Additionally, the DPO-MA must ensure that all reported critical asset vulnerabilities and remediation activities are sufficiently tracked and updated in the database.

g. The DPO-MA shall develop a Configuration Management Process for the purpose of integrating external comments into FSIVA documentation.

3.4 THE COMBATANT COMMANDERS

The Combatant Commanders shall be the point of contact in the identification of FSIVA requirements. Additionally, Combatant Commanders will provide liaison and coordination in support of the execution of FSIVA program requirements.

3.5 THE MILITARY DEPARTMENTS

The Military Department shall support the identification of additional FSIVA requirements. Additionally, the Military Departments will provide coordination and liaison in support of the execution of FSIVA program requirements.

3.6 THE DOD LEAD COMPONENT AGENCIES

The DoD Lead Component Agencies shall provide support to Combatant Commanders, the Military Departments, and assessment organizations in the coordination, liaison, and conduct of FSIVAs. Additionally, DoD Lead Component Agencies shall provide coordination and shall liaison with appropriate internal agency field activities, as required, in support of the FSIVA requirements.

3.7 THE DOD FSIVA PROGRAM ASSESSMENT ORGANIZATIONS

The DoD FSIVA Program Assessment Organizations shall coordinate and execute FSIVA Program Requirements in accordance with this CONOPs and other applicable directives and instructions.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

4.0 EDUCATION AND TRAINING

Conducting a FSIVA within the CIP capability area will require trained and experienced Subject-Matter Experts (SMEs) that are knowledgeable in CIP and the associated vulnerability assessment processes and standards. The staffs of DoD agencies that are charged with conducting vulnerability assessments currently include SMEs in several of the Areas of Concern identified in Appendix E. It is anticipated that several of these organizations may be asked to participate in performing FSIVAs. To ensure that the nuances of CIP and the assessment policies, processes, and standards are understood, the DPO-MA will develop a FSIVA Training Program for the CIP capability area. This training program will ensure that assessors from all supporting organizations are capable of meeting the full range of program requirements and performance standards associated with the CIP capability area.

5.0 CONCLUSION

The DoD CIP vision is to ensure that the critical infrastructure assets on which DoD depends are always available to mobilize, deploy, command, control, and sustain military operations. The vulnerability assessment is a necessary component of the overall DoD CIP Program and the Analysis and Assessment life-cycle activity. The FSIVA Program and associated CIP capability area standards provide assessment organizations with the necessary program guidance to assist them in conducting vulnerability assessments on assets determined critical by DoD. The results of the CIP capability area provide the Combatant Commanders, Military Services, and Defense Agencies with important information that is necessary in conducting a reliable risk assessment of their critical assets. Results of the risk assessment are key to decision-makers in developing valid recommendations for the remaining life-cycle activities. The CIP capability area provides DoD with a capability that assists Combatant Commanders, Military Services, and Defense Agencies in managing risk to critical assets that support their missions.

As directed by ASD(HD) and in consult with the Joint Staff (DDGO-AT/FP), the DPO-MA, with active participation from the DoD CIP community, will continue to develop the FSIVA Program and associated standards.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

APPENDIX A

CRITICAL ASSET NOMINATION AND PRIORITIZATION CRITERIA

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

As a part of the overall prioritization process, nominating criteria must be established. Prescribed nominating criteria would afford the commands, services, and agencies a mechanism for selecting and recommending critical assets for a FSIVA within the CIP capability area. In order for critical assets to be considered for a FSIVA, the critical assets should be rooted in an analysis of the following areas:

- a. **DoD missions** deemed most critical to national security, as articulated in the NMS.
- b. The **capabilities** required to successfully complete those missions.
- c. The **impact of the loss** of any of those critical assets on the successful completion of the mission.

The three areas of analysis listed above provide the broad categories against which each asset might be measured when being compared and prioritized against other nominated critical assets for FSIVA consideration. The use of prescribed definitions for respective priority levels within each of these categories (i.e., mission, capability and impact of asset loss) would support the measurement of an asset and enable a general prioritization of assets for FSIVA consideration. Armed with the results of this type of valuation process, the DPO-MA would be able to make informed decisions regarding the selection of assets for assessment and the allocation of finite FSIVA assessment resources, including personnel, time, and funds.

One example of what the priority levels might reflect in a given category is listed below.

IMPACT OF ASSET LOSS

Priority Level 1: Loss of the asset will cause a catastrophic loss of capability that cannot be replicated or provided by any other system in less than 120 days.

Priority Level 2: Loss of the asset will cause a severe loss of capability but may be replicated or provided by another system that can be available within 90-120 days.

Priority Level 3: Loss of the asset will cause a moderate loss of capability but may be replicated or provided by another system that can be available within 61-89 days.

Priority Level 4: Loss of the asset will cause an intermediate term loss of capability but may be replicated or provided by another system that can be available within 31-60 days.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

Priority Level 5: Loss of the asset will cause a short-term loss of capability that can be replicated or provided by one or more systems within 30 days.

In this example, it is envisioned that priority levels would be established for each of the three other categories of analysis using distinct and prescribed definitions for each area.

Upon receipt of asset owner nominations that include the appropriate information based on the nomination criteria, the DPO-MA will conduct a comparative analysis of all nominated assets using similar criteria but will be based on an overall DoD perspective that is rooted in the NMS.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

APPENDIX B

ASSESSMENT METHODOLOGY FOR THE CIP CAPABILITY AREA

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

B.1 FSIVA TEAM GUIDANCE

The CIP capability area assessment teams will be composed, organized, trained and equipped to conduct FSIVAs.

B.1.1 Team Composition

The CIP capability area teams will be composed of SMEs in the full range of areas of interest identified in the CIP capability area standards.

B.1.2 Team Member Training

Team members should possess an appropriate combination of knowledge, skills and experience to carry out their assessment responsibilities. It is required to have the assessment team members highly knowledgeable in the CIP capability area standards.

The assessment team must have a working understanding of all activities (analysis and assessment, remediation, indications and warning, mitigation, response, and reconstitution) in the DoD CIP Program and of the FSIVA standards and assessment methodology/process. Additionally, the assessment team must also have a collective understanding of the critical asset that is accurate and complete and must be able to communicate its understanding to others during and after the assessment.

B.1.3 Procedures for Handling Critical Infrastructure Information

Team members will have a minimum of a Secret level clearance and will be trained in accordance with the procedures set forth both in the *“DoD CIP Security Classification Guide”* and established DoD security guidelines.

B.2 STEPS IN THE FSIVA PROCESS

B.2.1 FSIVA Tasking

- Assessment team receives assessment authorization directive from DPO-MA.
- Directive identifies and establishes context of the designated critical asset, including known interdependencies.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

- DPO-MA schedules assessment and alerts assessment team of assessment dates and points of contact.

The assessment team will receive a directive to conduct a FSIVA in the CIP capability area on a designated critical asset from the DPO-MA after the critical asset identification and prioritization process have been completed. Critical assets selected for a FSIVA will have met all nomination criteria established by the DPO-MA.

B.2.2 Pre-assessment Requirements and Processes

Pre-assessment requirements and processes are currently under development.

B.2.3 Team Advance Preparation

- Study available read-ahead documents (e.g., mission statement, policies, design plans, analyses of known dependencies, etc.).
- Conduct Internet searches.
- Study available general intelligence data.
- Transmit clearances.
- Coordinate access requirements.
- Provide additional administrative/legal coordination.

In preparation for the CIP capability area vulnerability assessment, the assessment team will conduct a detailed review of the supporting analysis that lead to the identification of the critical asset. During this step, the team will review and study the analysis of the critical asset and its supporting infrastructure to gain a familiarity with the critical asset, the environmental context in which the critical asset functions, and some understanding of the direct and indirect impact of critical asset loss. This review will be performed in conjunction with the client/asset owner to ensure that the assessment team analysts fully understand the operational context associated with the critical asset. Additionally, during this step the assessment team will begin the preparation and refinement of specific checklists to be used by the team members in the assessment process.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

B.2.4 Team Final Preparation

- Team assessment mission-focused training (i.e., mission briefing) and integration of team assessment plans; identify probable cross-walk areas.
- Final team logistics preparation/confirmation of assessment support.

As part of the final team preparation, specific orientations, briefings, or specialized training is conducted as required by the nature of the critical asset and the environment in which it is being assessed. In the case of an Other Than Continental United States (OCONUS) FSIVA mission, this will include area of responsibility (AOR) security and travel briefings. Assessment team members conduct a final crosswalk of assessment plans to ensure all assessment areas are addressed and any potential areas of concern are identified for special focus as appropriate. The team completes all logistical support requirements, including those requirements for travel in designated overseas areas.

B.2.5 Team Pre-Assessment Visit

- Confirm mission/role and concept of operation.
- Conduct “Windshield tour” of facility.
- Confirm assessment scope, timelines, and team requirements.
- Obtain additional documentation.
- Identify/coordinate with asset owner’s liaison to assessment team.
- Identify/confirm report recipients and coordinate clearance requirements.

Select members of the assessment team conduct a preliminary site visit to obtain additional information regarding the critical asset, to confirm the scope of the assessment, and to verify the specific personnel and/or equipment resources that the assessment team will require to complete the assessment. This preliminary site visit will be conducted by two to three members of the larger assessment team and will include a “windshield tour” of the critical asset. Information obtained during the visit will be used to support the assessment team’s detailed preparation, including refinement of specific standards checklists, data gathering tools that the team will employ in the FSIVA process.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

B.2.6 On-site Assessment Requirements and Processes

On-site assessment requirements and processes are currently under development.

B.2.6.1 Conduct On-Site Assessment

(10-20 team members, 1-4 weeks depending on the nature of the critical asset and scope of assessment)

B.2.6.2 Verify Impact of Asset Loss or Disruption

- Identify/account for unanticipated redundancies.
- Assess the operational impact of the loss of the asset.
- Provide a factor that will assist in a quantifiable assessment of vulnerability.

This step begins the actual on-site FSIVA within the CIP capability area. Based on the preparatory research conducted previously, the entire assessment team will be oriented on the critical asset site, the critical asset's operational environment and its supporting infrastructure. The assessment team will review the analysis of the critical asset conducted previously by the asset owner as part of the critical asset identification process and the team will take note of the documented impact of critical asset or supporting infrastructure loss as the first element in the overall risk measurement. A mathematical factor representing the impact of asset loss will be assigned that will contribute to the measurement of risk later in the FSIVA process.

B.2.6.3 Assess Threat

A Threat Assessment Methodology is currently under development.

- Conduct threat analysis that examines full range of threat including conventional, terrorist, criminal, insider, cyber, weapons of mass destruction (WMD), naturally occurring threats and "other" potential threats attributable to factors unique to the environment.
- Threats will be linked to undesirable events.
- Threat assessment will consider capability, intent, and demonstrated history of actions.
- Obtain information via interviews with national and/or local law enforcement agencies (LEAs) and intelligence organizations.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

- Conduct internet searches.
- Adopt an adversary's perspective.

In this step the FSIVA team identifies and documents all of the potential threats that would result in undesirable events that can be reasonably associated with the critical asset and its supporting infrastructure. During this step, FSIVA team analysts identify and list a range of potential undesirable events, including man-made and naturally occurring events, and any known or potential threats that are capable of causing these undesirable events to occur. For man-made events, an analysis of the intent, motivation, capability, and demonstrated history of all potential threat organizations and/or individuals will be performed. For naturally occurring events, historical data regarding all types and occurrences of recurring natural phenomenon that could adversely affect the critical asset will be reviewed. Special attention will be focused on determining the specific weapon of the threat capability that inflicts the damage resulting in an undesirable event (the Damage Mechanism). Additionally, an assessment of the relative likelihood of potential accidental disruptions will be made from a review of the conditions of the critical asset's local environment. The overall threat level will be a relative rating based upon the analysis of each of these broad categories of threat. This step will produce a measure of the threat as the second element of risk measurement.

B.2.6.4 Assess Vulnerabilities

- Conduct vulnerability assessment including areas of physical security, cyber security, personnel, supporting infrastructure, supporting materiel and services, and planning and programs.
- Identify vulnerabilities through interviews, physical examination, and cross-walking observation data across the areas of assessment noted above.
- Identify any additional dependencies or previously unidentified redundancies.

The objective of this step is to identify critical asset and supporting infrastructure vulnerabilities that may be exploited by an identified threat and to produce a quantified measure of the relative vulnerability of the critical asset to any of the identified threats. All assets are susceptible to certain Damage Mechanisms and thus are protected by design factors and countermeasures to prevent Damage Mechanism access to the asset. The combined effects of these susceptibilities and countermeasures define the asset vulnerability. Vulnerabilities can be thought of as "pathways" to an asset. The

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

vulnerability of an asset is determined by the degree to which those “pathways” are “open” or are interrupted by existing countermeasures. Vulnerabilities to a critical asset can result from a wide variety of areas such as critical asset design and construction characteristics, environmental factors, proximity to other structures or systems, equipment properties, factors influencing accessibility, personal behaviors of people working in or around critical assets, or operational and personnel practices associated with the critical asset. The vulnerability assessment will focus on the actual, rather than the hypothetical vulnerabilities associated with the critical asset. Existing countermeasures that are in place, to include any that are physical, cyber or plan oriented in nature, will be analyzed to determine their relative degree of effectiveness in reducing the identified vulnerabilities. Specific vulnerabilities that are uncovered as a result of this analysis will be identified and characterized. The assessment team will develop a vulnerability rating criteria to determine asset/activity vulnerability levels. This step in the assessment process will conclude the on-site portion of the critical asset vulnerability assessment. An informal, preliminary out-brief addressing the assessment team’s significant initial findings will be provided to the appropriate officials prior to the vulnerability assessment teams’ departure from the asset location.

B.2.6.5 Assess Risk

A Risk Assessment Methodology is currently under development.

- Quantify and prioritize risks based on integration of criticality of asset loss (i.e., impact), threat, and vulnerabilities.
- Use standard definitions of levels of impact loss, threat, and vulnerability to calculate overall risk ($R = I \times (.T \times .V)$).

During this step, the assessment team will compute the level of critical asset risk based on the previously assigned measures of critical asset loss or disruption, identified threats and observed vulnerabilities. Risk will be expressed as a function of the impact of critical asset disruption set against the susceptibility of a given vulnerability to a particular threat. Risk levels will vary with time, circumstances, and evolving nature of threats. Given an analysis of relative risk, critical asset owners will ultimately decide what constitutes an acceptable level of risk. Priorities for reducing risk will be determined by the critical asset owners, in conjunction with the DoD CIP Directorate, based on their determination of acceptable levels of risk.

B.2.6.6 Analyze Countermeasures

- Include policy, procedural, technical, staffing, and training.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

- Provide countermeasure recommendations.
- Provide rough order of magnitude (ROM) cost estimates for countermeasures.

As a result of the information collected and analyzed in the previous steps, countermeasure options will be identified and designed to remediate the identified vulnerabilities and reduce risk to an acceptable level, as defined by the critical asset owner in conjunction with the DoD CIP Directorate. To identify countermeasure options, the most effective sets of countermeasures for each of the identified undesirable events will be determined. The countermeasures will be defined in terms of the level of risk reduction they provide. Assessment team analysts will determine the estimated rough order of magnitude cost of each countermeasure option package. Once the estimated costs of the countermeasure options have been determined, a cost benefit analysis will be performed to determine which option(s) provides the best protection at the lowest cost.

B.2.6.7 Develop Initial Out-brief (On-site)

- Tailor reports to asset owner needs.
- Provide to asset owner and appropriate DoD CIP stakeholders (i.e., Defense Infrastructure Sectors) for review.

The assessment team will prepare and present an informal out-brief of the initial findings and conclusions developed from the observation data gathered during the on-site assessment visit and preparatory research. This initial out-brief will focus on issues that may be particularly time sensitive or for which conclusions may be drawn without the need for extensive analysis. Information provided in this initial out-brief should be largely pre-decisional and will be subject to confirmation based on a more detailed analysis of observation data following the site visit.

B.2.6.8 Prepare Final Reports

- “Hard” and electronic copies
- Supported by full documentation
- Reports include graphics, photographs, and blast effects analysis

The final step in the assessment will be the preparation of a report of the FSIVA assessment and analytical risk management process. The report will provide

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

assessment observation and measurement data on the critical assets assessed that support clearly defined, actionable conclusions and recommendations. Information contained in the report will be configured to support the identified CIP data repository and meet the prescribed requirements for data tracking, archiving and retrieval. The report will be provided in paper copy and/or electronic copy as desired and will be classified and marked in accordance with the CIP classification guide as required.

B.2.6.9 Issue Final Report (Within 30 days of Assessment)

- Report to asset owner, approved stakeholders; archive maintained by DPO-MA
- Report findings of infrastructure vulnerabilities entered into DoD CIP database
- DPO-MA synchronizes infrastructure vulnerabilities with sector lead agencies

The FSIVA team's objective will be to issue the final report within 30 days of the completion of the assessment. Vulnerability and remediation data contained in the report will be used in the Planning, Programming, Budgeting and Execution (PPBE) process to assist in the allocation of security funding for remediation purposes. Release of the report document will be based on the approval protocol adopted by the DoD CIP Directorate, DPO-MA and the designated approval authority. Release of the report will be in accordance with (IAW) guidelines established by the DoD CIP Directorate and DPO-MA for document control and access.

B.2.7 CIP Capability Area Follow-up Assessment Requirements and Processes

Follow-up assessment requirements and processes are currently under development.

As programmed and scheduled by the DPO-MA, follow-up support will be designed to assist the commander or asset owner in ensuring the remediation of prioritized critical asset vulnerabilities and the allocation and effective use of funding to support that aim. "Red teams" will assist the commander/asset owner in verifying the effectiveness of applied countermeasures.

- Follow-up visit within 180 days to assess effectiveness of applied remediation measures.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

- Validate, through the conduct of exercises and/or red team, the adequacy of the implementation of completed corrective actions and determine if additional measures will be required.
- CIP red team verifies and documents solutions implemented by asset owner.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

APPENDIX C

**FSIVA AREAS OF CONCERN FOR THE CIP CAPABILITY AREA
STANDARDS**

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

The CIP capability area is intended to take a “modular” approach to conducting a vulnerability assessment of a designated critical asset. The CIP capability area 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 CIP capability area 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 Supporting Infrastructure.

Depending upon the nature of the critical asset to be assessed, several of the assessment areas of concern and assessment topic and subtopic 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.

The following information, listed below, is an explanation of the FSIVA 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 included below in the following paragraphs.
- b. TOPIC and SUBTOPIC: These sections identify the lower level topics and sub-topics that are associated with each of the broad areas of concern.
- c. EXPLANATION: This section briefly describes what each topic or sub-topic 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 sub-topic area.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

- 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 sub-topic. 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. The specific Combatant Command, Service and Agency mission will dictate which references and recommendations may apply to the numbered standards.

The Areas of Concern listed and described below are intended to reflect at a minimum, the broad areas that a CIP FSIVA is concerned with assessing.

C.1 PHYSICAL SECURITY

Physical security includes a consideration of the full range of security counter measures designed to deny physical access by unauthorized individuals and thus safeguard a critical asset’s key resources, including personnel, equipment, information, and facilities against espionage, sabotage, damage, and theft.

C.2 INFORMATION SECURITY

The structure, objectives, resources, techniques, and technical and administrative measures that protect data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

C.3 PERSONNEL SECURITY

Personnel security includes a consideration of the processes by which individuals are determined to be eligible and are properly credentialed for access to critical asset facilities and, when necessary, classified information. For a non-classified environment, this would include background checks for all personnel—employees, contractors, and service providers.

C.4 INDUSTRIAL SECURITY

Industrial security includes that portion of information security that is concerned with the control of individual access to classified information in the custody of the U.S. industry. This includes the issuing of clearances/background checks, ID badges/credentials, and educating staff on these procedures.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

C.5 SAFETY

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

C.6 PLANS

Plans include a consideration of all documented procedures, guidance, and policies, crucial to the security of a critical asset. Plans include intelligence sharing and liaison programs with supporting and neighboring agencies and the dissemination of security intelligence information to the personnel assigned to operate the critical asset. Plans include preparation for responding to possible contingencies as well as aspects of consequence management after an incident has occurred, such as Continuity of Operations (COOP) plans and actions of first responders.

C.7 OPERATIONAL SECURITY (OPSEC)

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

C.8 NUCLEAR SECURITY

Includes a consideration of that part of security concerned with the protection of nuclear facilities and/or special nuclear material at both fixed sites and during transportation.

C.9 CHEMICAL SECURITY

Includes a consideration of that part of security concerned with the protection of chemical agents at both fixed storage sites and during transportation.

C.10 BIOLOGICAL SECURITY

Includes a consideration of that part of security concerned with the protection of and against biological germs or substances at both fixed storage sites and during transportation.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

C.11 SUPPORTING INFRASTRUCTURE NETWORKS

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 (e.g., gas, oil, electric), transportation networks (e.g., railways, roadways, airports, seaports), communications (e.g., telecommunications, wireless), and water (e.g., potable, waste).

C.12 COMMERCIAL RELATIONSHIPS

Commercial relationships include a consideration of potential vulnerabilities inherent in the supporting commercial supply chain activities that support critical assets, including contractual obligations during both peacetime and during potential 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.

C.13 THREATS

“Threats” captures the broad range of events, both existing and future, that could potentially threaten a critical asset. These threats may include but are not limited to a foreign, domestic, or natural entity capable of exploiting critical infrastructure vulnerabilities that could debilitate the defense and/or economic security of the U.S.

C.14 COUNTERMEASURE RECOMMENDATIONS

This category denotes whether or not countermeasure recommendations are provided by the assessor in the written vulnerability assessment report.

C.15 WEAPONS OF MASS DESTRUCTION

C.16 STRUCTURAL RESPONSE

C.17 EMERGENCY OPERATIONS

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

APPENDIX D

REPORTING REQUIREMENTS FOR THE CIP CAPABILITY AREA

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

As a precursor to this process, it is assumed that the DoD critical assets are identified and prioritized in accordance with a process established within the DoD CIP community.

The final FSIVA CIP capability area report will be delivered no later than 30 days after the assessment is completed and will be provided in both a hardcopy and softcopy format. A softcopy format will allow the required data elements to be easily imported into DoD CIP databases. The final reports will be classified, will follow the procedures that are established in the DoD CIP Security Classification Guide, and will be distributed to the asset owner and approved stakeholders. ASD(HD) and DPO-MA will also maintain an archive copy of the report.

D.1 REPORT CONTENT/ORGANIZATION FOR THE FSIVA CIP CAPABILITY AREA (WEB-BASED SYSTEM)

The assessment report will be composed of an executive summary and profile that has been developed from data collected by the assessment team as support for the findings and conclusions of the assessment. The written assessment report will be used for management notification and information, initiating corrective and preventative action, and documentary evidence. The final report will be delivered no later than 30 days after the assessment is completed. It will be classified in accordance with the DoD CIP Security Classification Guide, and distributed to the asset owner and approved stakeholders. The DPO-MA will also maintain an archive copy of the report. In addition, the softcopy report will be available in an electronic format that allows the information to be easily imported into other DoD CIP databases. A draft report outline is listed below.

D.2 EXECUTIVE SUMMARY

D.2.1 Asset Identification

The assessment organization must include the identification of the organization, installation, or facility; the critical asset that was assessed, the mission supported by the asset, and the dates and period covered by the assessment.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

D.2.2 Security Classification

The assessment organization must include a statement that justifies the classification of the assessment report and any applicable restrictions to distribution.

D.2.3 Objectives of the FSIVA

The assessment organization must provide a description of the overall purpose of the assessment.

D.2.4 Organization of the Assessment Team

The assessment organization must provide a brief identification of team members and staff members of the assessed organization who supported the team during the assessment.

D.2.5 Modules Assessed

The assessment organization must include a brief description of the FSIVA modules that were covered in the assessment.

D.2.6 Conclusions

The assessment organization must summarize the key findings and recommendations including the vulnerabilities and the mission impact if left unaddressed.

D.2.7 Noteworthy Items

The assessment organization must provide any high-level observations and potential items of concern that are worthy of mention but might not be significant enough to mention as a key finding.

D.2.8 Items for Further Action

The assessment organization must summarize existing problem areas and provide recommendations for follow up activities by the critical asset owner based on the information collected.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

D.3 BODY OF THE REPORT

The assessment organization must include the following information in the body of the FSIVA report.

D.3.1 Introduction

The assessment organization must provide the following information in the Introduction.

- a. Purpose
- b. Detailed Scope of the Assessment
- c. Significant Assumptions
- d. Limitations and Exceptions
- e. Special Terms and Conditions (such as whether independent assessments occurred simultaneously in conjunction with the FSIVA)
- f. Reason for Performing a FSIVA
- g. Mission Focus

D.3.2 Site Description

- a. Location/Lat-Long
- b. Site and Vicinity General Characteristics
- c. Asset Physical Description
- d. Cyber Connection
- e. Description of Structure, Roads, and Access to the Asset
- f. Use of Adjoining Properties

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

D.3.3 Asset Owner Furnished Information

- a. Prior Assessments
- b. Specialized Knowledge About the Asset
- c. Known Vulnerabilities
- d. Asset Owner/Occupant Information

D.3.4 Records Review

The assessment organization must provide:

- a. Fire Dept Reports
- b. COOP/COG
- c. Local Utilities
- d. Physical Setting Sources (i.e., maps, GIS graphics)
- e. Cyber Setting Sources (i.e., maps, telecommunications plans)
- f. Potential Sources of Threat

D.3.5 Site Assessment

- a. Information collected at the site.
- b. What was observed at the site.
- c. The overall environment of the site as well as specifics.

D.3.6 Interviews

- a. Asset Owner
- b. Site Commander
- c. Occupants

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

- d. Local Government/ Agency
- e. Regional Government/ Agency
- f. Others

D.3.7 Findings

- a. Summarize known vulnerabilities associated with the asset
- b. Dependency Diagrams

D.3.8 Impact

The team gives expert opinion of the impact on the critical asset of the known or suspected vulnerabilities. If the level of vulnerability can be quantified, then the team should list their conclusions in the conclusion section of the report.

D.3.9 Conclusions

Summarize all vulnerabilities connected with the asset and the impact to the mission if vulnerabilities are not addressed. Not all findings will necessarily be listed in this section.

D.3.10 Recommendations

The team gives expert opinion on best countermeasures that will remediate the identified vulnerabilities. Additionally, this section will talk about any potential new vulnerabilities that could be introduced when the original vulnerability is remediated.

D.3.11 Deviations

Explains why something normally in the report was not included or if something was added that is normally not part of the scope of work was included.

D.3.12 Additional Services

- a. Broader Scope

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

- b. Risk Assessment
- c. Remediation/Cost Estimates

D.3.13 References

Checklists/standards/best practices used in the assessment.

D.3.14 Qualifications for the Team

Team Bios (one paragraph summary of each team member).

D.3.15 Appendices

- a. Maps
- b. Plan
- c. Photos
- d. References - Checklist/standards/best practices used in the assessment
- e. Qualifications of the CIP FSIVA Team - Team member Bios (one paragraph summary per team member)
- f. Data Element Requirements for CIP Database
- g. Any additional documentation

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

APPENDIX E

DATA ELEMENT REQUIREMENTS FOR THE CIP CAPABILITY AREA

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

The table below lists the minimum required CIP assessment data elements and their descriptions. This information is required for every assessment that is conducted and will be used to populate the CIP Database.

<i>Required Data Element</i>	<i>Definition</i>	<i>Description</i>
Critical Asset	Critical Assets are those assets, which if delayed, lost or destroyed would significantly disrupt/adversely affect one or more aspects of DoD operations during specified mission scenarios and periods of time.	Name of asset, asset mission description, and type of asset (Force, Base/Port, Facility, System, Equipment, Resource, Service/Agency, or Infrastructure)
Supporting Assets	Any resource, military or civilian, CONUS or OCONUS, instrument, installation, or system for use in a military operational or support role. Assets include traditional "physical" facilities, units, or equipment; non-physical assets (such as software systems); or assets that are distributed in nature (such as assets within command and control networks, wide area networks or similar computer-based networks).	Name of asset, asset mission description, and type of asset (Force, Base/Port, Facility, System, Equipment, Resource, Service/Agency, or Infrastructure)

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

<i>Required Data Element</i>	<i>Definition</i>	<i>Description</i>
Point of Contact		<ol style="list-style-type: none"> 1. Name 2. Title/Rank 3. Command, Agency, or Company 4. Office Code 5. Commercial and DSN Phone Number 6. JWICS, SIPRNET, and NIPRNET Email Addresses 7. DMS Address 8. Plain Language Address Directory 9. Mailing Address
Asset Location		<ol style="list-style-type: none"> 1. Street Address 2. Building/Facility Number 3. City 4. State/Region 5. ZIP Code 6. Country 7. Latitude and Longitude Data (degrees/minutes/seconds)
Dependencies	<p>When one system or asset has a dependency upon other systems or assets within another or the same infrastructure in order to support DoD Mission requirements. This includes intra-dependencies from systems and assets from the DoD segment of the infrastructure to the Commercial segment with another or within the same infrastructure.</p>	<p>Provide the name of the asset(s) depended upon. Also, provide narrative description of the dependency and the impact upon the asset if dependency were lost.</p>

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

<i>Required Data Element</i>	<i>Definition</i>	<i>Description</i>
Mission Impact	Impact on a mission due to the loss or degradation of either mission required or infrastructure supporting critical assets.	Provide a narrative description of the operational mission impact if the asset were lost.
Vulnerability	The characteristics of a system which causes it to suffer a definite degradation as of a result having been subjected to a certain level of hazard effects from both natural disruptions and unnatural, or manmade hostile environment (i.e., terrorists attacks). Maybe physical or cyber vulnerabilities.	Provide a narrative description of each of the vulnerabilities
Threats	A threat is any real or potential condition that can cause an adverse effect. The condition can be natural or unnatural events. A threat is a foreign, domestic, or natural entity capable of exploiting critical infrastructure vulnerabilities and that could debilitate the defense and/or economic security of the U.S.	Provide a narrative description of threat.
Remediation	Identification of and assessment of continuity of operations plans	Provide a narrative assessing existing remediation plans available in event of loss of asset. Provide plan location and POCs. Provide status of remediation efforts to known vulnerabilities.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

<i>Required Data Element</i>	<i>Definition</i>	<i>Description</i>
Recommended Remediation Actions		Provide narrative description of the remediation options for each identified vulnerability.
Indications and Warning	Domestic criminal activity, environmental, weather, or signs that technical anomalies, system failure, or degradation is likely, planned, or is underway. Warning is advance notification that technical anomalies, system failure, or degradation is likely or planned.	Provide narrative description of the capabilities for monitoring and reporting vulnerability information. Provide a list of indications and associated warnings of a threat exploiting a vulnerability.
Mitigation Plans	Plan of actions taken by the defense infrastructure sectors and by military operators in response to an infrastructure warning, vulnerability, or incident.	Provide narrative description of the existing mitigation plans (COOPs) available in event of loss of asset. Provide plan location and POCs. Provide status of mitigation efforts to known vulnerabilities.
Recommended Mitigation Actions		Provide narrative description of the mitigation options for each identified vulnerability.
Response Plans	Plans that guide activities undertaken immediately to eliminate the cause or source of an adverse event. Actions taken in response to an undesirable or emergency situation, including emergency measures from dedicated third parties such as medical, police, and fire and rescue for public safety.	Provide narrative description of the third party response plans in event of loss of asset. Provide plan location and POCs.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

<i>Required Data Element</i>	<i>Definition</i>	<i>Description</i>
Reconstruction Plan	Plan of actions required to rebuild or restore an aspect or portion of an infrastructure after it has been degraded.	Provide narrative description of the plans for reconstruction of infrastructure, asset, or system in event of loss of asset. Provide plan location and POCs.

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

APPENDIX F
AFTER-ACTION REPORT REQUIREMENTS

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

1. Cover (standardized cover with appropriate classification as required)
2. Table of Contents
3. Introduction
 - a. Assessment Objective
 - b. Purpose of Report
 - c. Organization of Report
4. Executive Summary
 - a. Lesson's Learned (significant)
5. Discussion
 - a. Name of Assessment
 - b. Dates
 - c. Site/Location
 - d. Site/Location Primary POC
 - e. Assessment Team Lead
 - f. Team Construct (Name/Organization(s))
 - g. Modules (Areas Of Concern/standards) addressed
 - h. Tools utilized in support of assessment and description
 - i. Concept of Operation
 - (1) What was suppose to happen
 - (2) What happened
 - (3) Why it happened, and how to improve
 - j. Out-brief (attendees/remarks/comments)
 - k. General Comments
6. Summary of Observations (summary and complete list of lesson's learned)

**For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations**

APPENDIX G

TRACKING PROCESS FOR THE CIP CAPABILITY AREA

For Official Use Only
FSIVA Program
CIP Capability Area Concept of Operations

These data fields should provide managers at various levels the information required to effectively schedule FSIVA, track the progress of vulnerability remediation, and evaluate the benefit of funds committed to vulnerability remediation, as determined by the change in measured levels of risk.

1. Coordination and Scheduling

- a. Name and location of critical asset
- b. Date of previous FSIVA
- c. Scheduled date of next FSIVA
- d. Actual date FSIVA occurred
- e. Projected follow-up visit
- f. Date of follow-up visit

2. FSIVA Results

- a. Number of vulnerabilities identified listed by categories of degree of severity (e.g., Critical, High, Medium, etc.)
- b. Areas of vulnerability (e.g., closed-circuit television (CCTV), lack of adequate firewalls, lack of plans, etc.)
- c. Date of remediation
- d. Type of countermeasure installed

3. Follow-up Results

- a. Number of new vulnerabilities identified, as a result of the remediation effort, listed by categories of degree of severity
- b. Areas of new vulnerability (e.g., CCTV, lack of adequate firewalls, lack of plans, etc.)
- c. Change in measured risk level based on remediation of initial vulnerabilities and consideration of new vulnerabilities

4. Program Funding

- a. Maximum and minimum cost estimates for remediation of initial FSIVA vulnerabilities
- b. Maximum and minimum cost estimates for remediation of new vulnerabilities
- c. Remediation funding requested, by year
- d. Remediation funds received, by year
- e. Funds committed to vulnerability remediation, by year