U.S. Department of Energy

Cyber Security Program

REVITALIZATION
# of the
DEPARTMENT OF ENERGY
CYBER SECURITY PROGRAM

February 2006

Version	Revision Date	Description/ Change
0.1	01/19/06	Initial incomplete outline
0.2	01/26/06	Added outline and rough draft of text for section 3; modified section 4 to reorder sequence of activities to align activities with budget cycle.
0.3	02/09/06	Replaced sections 1 and 2; replaced section 3 text; rough draft of section 5; separated document into two volumes.
0.9	02/14/06	Removed separation of document into two volumes; added introduction section to explain overall plan contains two phases; added new section 3 to describe phase 1 activities.
0.95	02/17/06	Significant restructuring of contents to reflect multiple initiatives within overall plan; added draft Executive Summary; reordered Roadmap section to arrange material following cyber security component list.
0.96	02/20/06	Numerous minor corrections to text; inserted new guidance and cyber security activities in section 7; inserted text to replace all TBDs.
0.97	02/21/06	Integrated DOE CIO's initial comments.
0.99	02/2206	Corrected typos and minor errors; added section on implementation and resources
1.0	02/24/06	Final Version
1.1	03/08/06	Move appendices A and B to an OUO attachment.

Table of Contents

Table of Figures

Executive Summary

Cyber security is a difficult challenge in an era where threats to the Department's information and information systems are constantly evolving. The Department of Energy (DOE) faces significant challenges in implementing and maintaining a comprehensive cyber security program that is effective across its diverse missions and large array of interdependent networks and information systems. Over the past several years, internal and external assessments of DOE's unclassified cyber security program have repeatedly identified significant weaknesses in the information and information systems vital to Departmental missions and operation.

Priority attention must be institutionalized throughout the Department, including all aspects of how the Department conducts its business and serves the citizens. People, processes, and technology must be leveraged to have an effective program. Cyber security, like safety, quality, and fiscal prudence is a cornerstone of good operations. The Department has identified systematic ways to integrate cyber security into our missions so that risks are effectively managed and monitored. Over the next 12 months the DOE Chief Information Officer (CIO), in coordination with the Under Secretaries (including the National Nuclear Security Administration (NNSA) Administrator), the Energy Information Administrator, the Director of Security and Safety Performance Assurance, and the Power Marketing Administration (PMA) Representative), will lead the implementation of a comprehensive program with activities that address the systematic improvement of the Department's capabilities. The cyber security program will be structured to meet the anticipated and unforeseen challenges based on the strength of the Department's people, processes, and technologies. This program addresses weaknesses in the Department's cyber security posture as well as mitigates the more immediate issues identified by independent assessments/audits such as those by the Inspector General and the Office of Safety and Security Oversight.

The course of action outlined in this plan is based on a series of principles derived from the Department's experience in implementing past corrective recommendations, extensive assessment of the current situation by the Office of Chief Information Officer (OCIO), and discussions among the Deputy Secretary, the Under Secretaries, the OCIO, and the staff office representatives, and lessons learned within the Federal government. The following three principles run throughout the plan described in this document and guided its development. Specifically they are:

1. Managing cyber security risk in a dynamic threat environment requires managing and sharing information. This management is built on clear priorities and requires sharing threat information and lessons learned to maximize program benefits. Managing risk should be performed based on cost avoidance and effective use of resources in such a manner as to be "sufficient but not overdone".
2. Cyber security is everyone's business. The Under Secretaries are key players, responsible for ensuring adequate protection of systems and data within their organizations, and, also identifying and applying the necessary resources to do so. The cyber security program's roles and responsibilities are distributed among senior Department leaders to ensure a strong cyber security posture, while preserving mission capability. Therefore, the OCIO sets priorities and requirements through high-level policy and guidance, while the

Under Secretaries are responsible for detailed policy and guidance and implementation in their organizations. The Under Secretaries tailor the OCIO-provided guidance and baselines to their mission. OCIO focuses on leadership and support of a comprehensive program that provides a proactive approach to mitigating the security threat to the Department, enables the continuous monitoring of the cyber security posture, and supports a wide range of cyber security services supporting implementation of the program.

3. The revitalization plan systematically upgrades the DOE cyber security posture over twelve months, providing a strong beginning to long-term revitalization. The plan is designed to strengthen the Department's networks and establish a vital, institutionalized cyber security program. The approach is built on quickly deploying and institutionalizing activities in five high priority areas, listed below. These will initiate positive changes that are encompassed in the longer term activities:
    a. Certification and Accreditation Assistance
    b. Enterprise Defense-in-Depth Strategy
    c. Asset Management
    d. Network Interconnection and Segmentation
    e. Education and Awareness Program

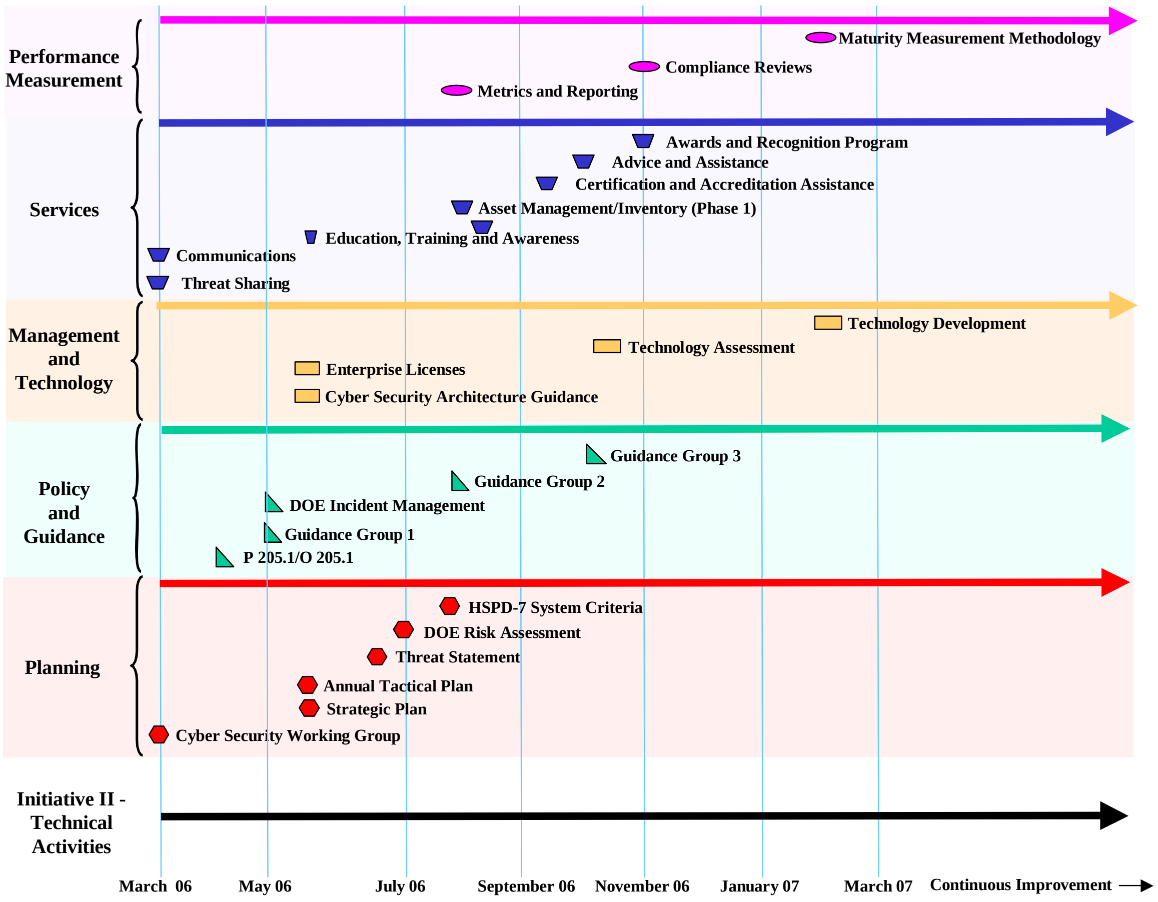
The longer term cyber security program is composed of several components, including planning, policy, management and technology, services, and performance management, described below. However, it is the mutually reinforcing nature of these elements of cyber security, which emphasize the need for a strong governance structure for the cyber security program. This governance structure allows senior leadership to see across the program and coordinate with each other across the Department; places responsibility and accountability at appropriate levels; and sets, measures, and rewards performance.

- Planning – Planning is supported by a collaborative effort to understand the threat landscape and identify weaknesses through compliance reviews and performance measurement. This information is fed back into the planning activities to generate both a long-term strategic plan and an annual tactical plan. Processes and artifacts produced include cyber security working group, strategic and tactical plans, and both a Departmental threat statement and risk assessment.
- Cyber security policy and guidance – The policy component is very closely aligned with both the governance program and the planning component. Cyber security policies establish the high-level goals and outcomes for the overall DOE Cyber Security Program. Enhanced through guidance, and performance metrics, the policy is in place to drive the program's implementation. The focus is on top-level "thin-policy" supported by guidance at the Departmental level.
- Architecture and Technology – Installing well-defined, high-level Department structure, processes and principles puts the Department in position to successfully manage the technology it employs. To achieve the best possible results from this structure and to ensure that a standard approach across the Department is achieved, the set of sub processes, which fall within the Leadership Decision process, address the man-

agement and technology component. Artifacts stemming from this component include architectural guidance, enterprise licensing of security tools and products, and a technology review and development process.

- Services – Sizeable changes to any organization can be difficult. As Under Secretary and Program Offices adapt to the new processes and policies, it is the role of the OCIO to facilitate that adjustment thorough various services and through the performance of several key initiatives that protect the entire Department. The aim of these programs is to develop an intelligent, proactive approach to mitigating the security threat to the Department and other Agencies. Processes stemming from this component include cyber security communications, education and awareness, asset management, advice and assistance, and awards and recognition.
- Performance Measurement – Performance measurement provides a clear and consistent way to measure success and demonstrate results for senior management. Process and artifacts stemming from this component include compliance review and monitoring and cyber security metrics.

A high-level schedule for initial OCIO and Undersecretary work on these components is provided below. Only the major OCIO milestones for the next twelve months are shown, continuous improvement of the DOE Cyber Security Program will occur throughout the entire program.



The OCIO will begin work immediately under this Revitalization Plan and will leverage existing intellectual capital within DOE and best practices drawn from both within and outside the Department. The OCIO will implement a series of high impact/priority activities in parallel to the institutionalization of the revitalized cyber security program. The OCIO activities described in this document are not a short campaign and the 12 months covered by this plan are only the beginning if DOE is to institute a successful cyber security program.

The role of the Under Secretaries is also critical to the success of cyber security at DOE. The Under Secretaries are responsible for the development and implementation of a cyber security framework for their organization. This framework addresses the tailoring and implementation of policy and guidance to support the Under Secretary organization; enhancement of their Program Cyber Security Plan; and providing direction to subordinate Federal and contractor organizations. The responsibilities of the Under Secretaries also include implementing the appropriate aspects of the high priority activities identified by the OCIO, based on risk and mission. A fundamental role of the Under Secretaries is to ensure long-term, continued emphasis on cyber security, including the identification and commitment of required resources needed to support the implementation of the Department's revitalized cyber security program within their organizations.

1. Introduction

The Department of Energy (DOE) faces significant challenges in implementing and maintaining a comprehensive cyber security program across its diverse missions and large array of global networks and information systems. Over the past several years, internal and external assessments of DOE's unclassified cyber security program have repeatedly identified significant weaknesses in the management processes and operational controls relied upon to protect the confidentiality, integrity, and availability of the information and information systems vital to Departmental missions and operation. Substantial work must be accomplished to improve the cyber security posture of the Department and revitalize the DOE Cyber Security Program.

This plan to revitalize the DOE cyber security posture and program was initiated by the DOE Office of the Chief Information Officer (OCIO) in response to recent cyber incidents and the significant weaknesses in the Department's cyber security program. This plan was coordinated by the DOE OCIO organization and developed in collaboration with the Cyber Security Working Group (CSWG) under the oversight of the Cyber Security Executive Steering Committee (ESC).

Figure 1 provides an overview of the overall approach of this plan to revitalize the DOE Cyber Security Program. The figure depicts the efforts already underway at DOE Headquarters and the National Nuclear Security Administration (NNSA) Service Center, the

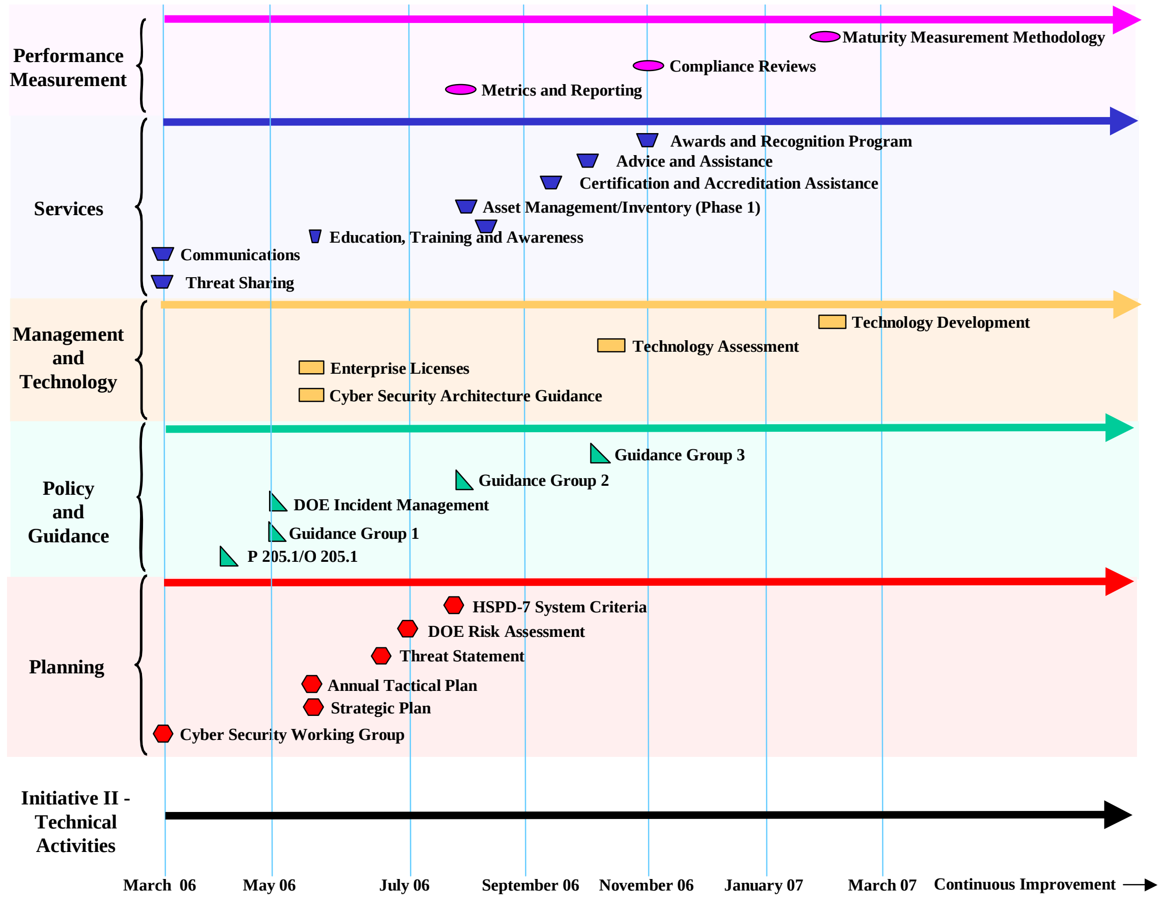


Figure 1. Revitalization Plan Overview

immediate and short-term remediations recommended by the Cyber Security Project Team (CSPT) and the DOE OCIO, and the long-term strategy to improve the Department's cyber security program to achieve world-class protection and apply best practices to protect the Department's information and computing assets. Only the major OCIO milestones for the next twelve months are shown, continuous improvement of the DOE Cyber Security Program will occur throughout the entire program.

Section 2 of this plan provides an overview of the path forward to accomplish this revitalization effort. Section 3 identifies the drivers for creating this revitalization plan and gives the reader background information to help explain why the Department initiated the development of this revitalization plan.

The activities in revitalizing the DOE cyber security program are divided into three distinct but inter-related initiatives. Initiative I, described in section 2.2.1, includes a number of critical remediation activities, including several recommendations identified by the Cyber Security Project Team (CSPT), which required immediate deployment to shore up the Department Headquarters, the National Nuclear Security Administration (NNSA) Service Center, and the National Training Center (NTC) infrastructure. Initiative II, described in section 2.2.2, includes the immediate and near-term actions needed to address Department-wide issues identified during recent red team activities.

Initiative III, described in section 4, includes activities designed to address the longstanding systemic cyber security management issues facing the Department through institutionalizing fundamental changes in DOE's governance related to cyber security. The proposed governance structure and program components (planning, policy, management and technology, services, and performance management) are closely coupled to provide both a clearly defined mechanism for decision-making and aid in ensuring the alignment and integration of cyber security capabilities and services, as well as, the clear delineation of cyber roles and responsibilities. Section 4.2 contains a high-level description of the contents and operation of the revitalized cyber security program. Section 4.3 describes the components of revitalized cyber security program. Section 5 contains the roadmap and description of the activities needed to establish and institutionalize the revitalized cyber security program.

2. Overview

2.1 Background

The missions of DOE are perhaps more diverse than any other agency of the U.S. Government. These missions are performed at geographically dispersed sites, primarily utilizing government-owned, contractor-managed facilities. Information technology support is provided by a geographically separate, interconnected group of computing enclaves. To manage the often disparate missions, DOE has historically utilized a federated information technology management approach.

Under this federated approach, on behalf of the Secretary, the OCIO provides cyber security policy guidance to the Under Secretaries, the Administrator of the NNSA, and DOE staff offices. Each line management chain integrates this policy into a Program Cyber Security Plan (PCSP) tailored to their specific mission and risk environment.

Recognizing that the variety of missions and federated nature of the DOE can pose a significant challenge to ensuring the security of the Department's computing systems and information assets, the OCIO is actively addressing the need to meet the necessary regulatory and federally mandated requirements to ensure the protection of DOE unclassified and classified assets and information. With a significant effort on revitalizing the DOE Cyber Security Program, the OCIO is focused on creating a flexible program that can address the threats of today and tomorrow.

Substantial work must be accomplished to revitalize the DOE Cyber Security Program. An aggressive goal of implementing a revitalized program in the span of 12 months is achievable through implementing the roadmap defined in section 4 this plan. Utilizing this roadmap as a high-level implementation blueprint in combination with the program structure outlined in section 4 over the next 12 months, the OCIO will implement a comprehensive program of capabilities and activities that address the systemic weaknesses in the Department's security posture as well as mitigate the more immediate issues identified by independent assessments/audits such as the CSPT.

2.2 Immediate Activities Supporting the Revitalization Plan

As the OCIO works with the Under Secretaries and other Departmental stakeholders in creating a stronger and increasingly effective Department-wide Cyber Security Program, there are critical issues, which require immediate attention. These weaknesses in the Department's cyber defenses, brought to light by recent audits and network incidents, require a more rapid response while the revitalized program is implemented. These weaknesses require urgent attention and action by both the OCIO and Under Secretary organizations.

2.2.1 Immediate Remediation Activities at HQ, NNSA Service Center, and NTC

Prior to the development of the revitalization plan, a number of activities were identified by the CSPT that the OCIO determined required immediate deployment to shore-up the Department's IT infrastructure and remediate critical weaknesses. Implementing these immediate remediation activities and selected CSPT recommendations was initiated immediately, and implementation is continuing as "stop gap" measures. Upon the acceptance of the revitalization plan, these activities are intended to be integrated into Initiative II. A complete listing of those activities and their status is provided in Appendix A in the Official Use Only attachment to this document.

2.2.2 Technical and Operation Issues within the Under Secretary Organizations

All of DOE is affected by the significant weaknesses identified through the recent internal and external assessments of DOE's unclassified cyber security program. Initiative II identifies a number of high impact areas of concern identified by the OCIO. These mitigating actions for the high impact areas are primarily split between the OCIO and Under

Secretaries; however, coordination is essential for the successful execution of responsibilities by both organizations. The OCIO has primary responsibility for Department wide issues related to cyber security program policy and management, while the Under Secretaries' emphasis is on operational and technical items. However, the OCIO has direct management responsibility for the DOE infrastructure (DOEnet) and the federal "Most Efficient Organization" under the recent A-76 contract award. As such, the OCIO will act as the vanguard for the Department in executing against these high impact objectives. Through implementing mitigating actions in these areas, DOE will recognize immediate improvement in the cyber security posture of the Department's Information Technology (IT) infrastructure. The areas of concern, mitigating actions, and their status are identified in Appendix B in the Official Use Only attachment to this document.

2.3 Moving Forward

The need to establish a superior cyber security program is, in part, driven by a variety of recent internal and external assessments of DOE's unclassified cyber security program that have identified significant weaknesses. All organizations within DOE are affected by these discoveries and all elements of the Department must work together to strengthen the security of the Department.

The OCIO will begin work immediately under the Revitalization Plan provided in this document. As the OCIO leads the establishment of a robust cyber security program it will leverage existing intellectual capital within DOE and best practices drawn from both within and outside the Department. Close collaboration between the OCIO and the CSWG is critical to the success of this approach. To support rapid improvement in the DOE security posture the OCIO will implement a series of high impact/priority activities in parallel to the institutionalization of a revitalized cyber security program. The OCIO activities described in this document are not a short campaign and the 12 months covered by this plan are only the beginning if DOE is to institute a successful cyber security program.

The role of the Under Secretaries is also critical to the success of cyber security at DOE. Under Secretaries have a number of cyber securities related responsibilities. They are responsible for the development and implementation of a cyber security framework for their organization. This framework addresses the tailoring and implementation of policy and guidance to support the Under Secretary organization; enhancement of their Program Cyber Security Plan; and providing direction to subordinate Federal and contractor organizations. The responsibilities of the Under Secretaries also include implementing the appropriate aspects of the high priority activities identified by the OCIO, based on risk and mission. A fundamental role of the Under Secretaries is to ensure long-term, continued emphasis on cyber security, including the identification and commitment of required resources needed to support the implementation of the Department's revitalized cyber security program within their organizations.

3. Drivers and Background

DOE faces significant challenges in implementing and maintaining a comprehensive cyber security program across its diverse missions and large array of global networks and information systems. Over the past several years, internal and external assessments of DOE's unclassified cyber security program have repeatedly identified significant weaknesses in the management processes and operational controls relied upon to protect the confidentiality, integrity, and availability of the information and information systems vital to Departmental missions and operation. Consistent with these assessment results, DOE has been assigned a failing grade in cyber security by the Congressional Committee on Government Reform each of the last four years. Further, previous Secretarial-level initiatives launched in 2004 and earlier this year to improve DOE's cyber security posture have not achieved the desired improvements.

The Department's cyber security challenge has been made increasingly difficult not only by the generally recognized increase in the number and sophistication of threats to its systems, but also by improved internal performance testing that has identified real, but previously unsuspected, vulnerabilities.

The impetus for this initiative to revitalize the Department's cyber security program and practices include the results of recently-concluded unannounced network penetration testing (red teaming) conducted by Security and Safety Performance Assurance's Office of Independent Oversight (SP-40), determination of root causes for the poor grades assigned by the Congressional Committee on Government Reform, examination of audit and inspection results, and analysis of the increasing number and sophistication of the threats to Departmental information assets.

Based on past lessons learned and recognition that certain specific issues had a higher or more immediate impact on the security posture of the Department, the OCIO identified five high-impact management areas requiring special attention. Each of these initiatives addresses a significant cyber security issue across the Department and as such acts as a driver for the larger program.

- Certification and Accreditation (C&A) Assistance – create a more robust C&A process that assures all systems that support the missions of DOE are authorized and accredited with clear understanding of current risk and security posture on the part of senior management.
- Enterprise Defense-in-Depth Strategy – builds upon the current guidance of the DOE and ensures that security is addressed by all elements of the Department.
- Asset Management – identifying the assets and ensuring they comply with the security policies of the DOE and managing security to the lowest degree helps the DOE achieve a strong security posture.
- Network Interconnection and Segmentation – ensures that connected systems both within the DOE-enterprise and from other agencies have identified,

documented, and appropriate security postures to protect the data on both systems.

- Education and Awareness Program – educating and empowering the DOE security professional and user to take responsibility for the security of the Department through programs that build awareness throughout the Department.

4. Initiative III - Revitalized Cyber Security Program

4.1 Revitalized Cyber Security Program Overview

As the DOE cyber security program is revitalized, developing a refined cyber security governance structure and supporting components for the program is critical for ensuring that cyber-related decisions align with departmental goals. The governance structure and program components are closely tied to provide both a clearly defined mechanism for decision-making and aid in ensuring the alignment and integration of cyber security capabilities and services, as well as, the clear delineation of cyber roles and responsibilities. The program components are made up of a number or major processes and sub-processes that are addressed in detail within the following sections. The processes focus on providing a standard mechanism for the activities that fall under the program components.

An inherent benefit of a well-designed governance structure is increased efficiency and cost savings. This results from the coordination of the various cyber security program components and the enhancing effect on the Department's security posture brought about by the interconnection of processes associated with the program components, a federated approach implemented across all elements of the Department, and the coordination of cyber security with other aspects of IT management within DOE such as capital planning and e-Government. The cyber program outlined throughout the rest of this section is designed to achieve these benefits.

4.2 Program Governance

Governance for the cyber security program will reflect a maturing and refinement of the federated approach. The refined federated governance process, Figure 2, includes leadership by the OCIO together with the Department's Under Secretaries. OCIO and the Under Secretaries will continue to "partner" in cyber security through a Departmental Cyber Security Executive Steering Committee (ESC). The OCIO chairs the ESC with additional voting members consisting of the NNSA Administrator, the Under Secretary for Energy, Science and Environment, the Under Secretary for Science, the Administrator of the Energy Information Administration, the Director of Security and Safety Performance Assurance, and one Power Marketing Administration (PMA) Administrator. Each ESC member will identify an individual to be on the Cyber Security Working Group (CSWG), which will support the ESC.

The members of these groups create the Department's governance process. Without the support and coordination of their members, new policy and guidance would lack valuable insight derived from operational experience. The views expressed by the members of these two groups impact the future of the OCIO's Cyber Security Program and are essential in creating a secure future. The CSWG is the technical representation of the DOE executive leadership and therefore, advises and proposes changes in Departmental policy, methodologies, approaches, and realignment of capabilities (in compliance with national standards). The CSWG also assists the OCIO in assuring the adequate performance of the cyber security program at the DOE, including NNSA. The CSWG serves as staff for the ESC and supports the coordination and implementation of cyber security policy, technical, and operational activities across the Department. They work collectively to ensure that guidance meets the rigorous demands of the Department before being considered as DOE guidance by the ESC.

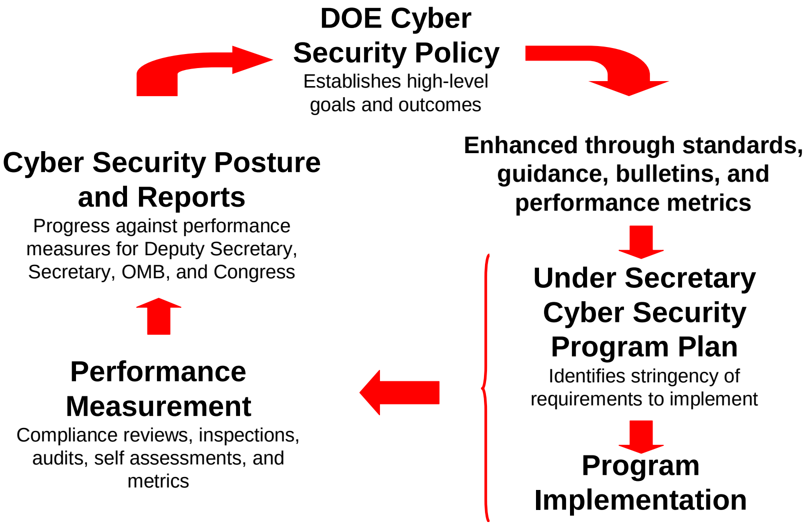

DOE Cyber Security Policy
Establishes high-level goals and outcomes
Enhanced through standards, guidance, bulletins, and performance metrics
Under Secretary Cyber Security Program Plan
Identifies stringency of requirements to implement
Program Implementation
Performance Measurement
Compliance reviews, inspections, audits, self assessments, and metrics
Cyber Security Posture and Reports
Progress against performance measures for Deputy Secretary, Secretary, OMB, and Congress

Figure 2. Cyber Security Program Governance Structure

While ensuring the security of DOE cyber assets and data through policy is of paramount concern to the OCIO, there is an understanding that not all missions or sites can operate under the same guidance. There exists a need and desire to retain flexibility in the program to both address security requirements and employ a solution that does not hinder the mission of the various sites that make up DOE. With that in mind, the OCIO has set upon the concept of utilizing top-level policy supported by guidance to drive the program. Using "thin" top-level policy affords the OCIO the ability to create and deliver policy that embraces the needs of the entire Department. To address the challenge of ambiguity and varied mission needs, while allowing the OCIO to establish high-level goals and outcomes through the issuance of top-level policy, the OCIO relies upon guidance, bulletins, and/or performance metrics to complement policy. The policy, supporting guidance, and metrics pieces are intended to clearly define the Under Secretary's responsibilities and enhance the downstream implementation by the Under Secretary organizations and Program Offices with the full support of the OCIO services.

While the OCIO is responsible for delivering high-level Departmental policy for Deputy Secretary approval and providing timely guidance products for Department-wide use, it becomes the responsibility of the Under Secretary to build from this a Cyber Security Program Plan that identifies the stringency of the requirements to be implemented within their organizations. This freedom allows the Under Secretary the capability to create a program that best suits the needs of their mission while ensuring that the baseline security requirements are addressed. This plan defines roles and responsibilities as well as minimal cyber requirements and baselines for implementation by the various elements of the Under Secretary organization

Validation of the Under Secretary and Program Office's ability to implement adequate security requirements is handled through the performance measurement attributes of the program. These attributes will include compliance reviews, inspections, audits, self-assessments, and metrics. All of these attributes, especially metrics, will be measured against the Departments baseline. The baseline is established by the afore mentioned guidance and bulletins, which provide the minimum level of compliance.

To ensure that the Department is measuring up to the established baseline and progressing towards a more secure operating environment, a repository of cyber security posture statements and reports will be made available to the highest levels of the DOE executive management. In addition to Department leadership, this information will be available for the Office of Management and Budget (OMB) and Congress. This information will clearly show the progress of the Department as applied to the performance measures and establish that the Department is moving in the direction of achieving its security goals.

The described governance structure (process) allows the OCIO to establish Department-level guidance that can in turn be followed explicitly or expanded upon to meet the variety of the DOE missions that exist among its sites and labs. In keeping with the Department's federated history, adopting this concept creates flexibility in policy and guidance while bolstering the security of the Department.

To achieve the best possible results from this structure and to ensure that a standard approach across the Department is achieved, the following set of supra-processes address program governance. In addition, these supra-processes encompass supporting sub processes within the individual program components. This further illustrates the critical tie between senior leadership through the governance role and executing the program through its components.

- Leadership Decision – this process incorporates all elements of the DOE leadership in the decision-making construct and allows for policy, guidance, and services concepts to be fully vetted as they migrate from general guidance to accepted guidance.

- Implementation – this provides the Under Secretaries with a process for implementing the policies and guidance approved through the Leadership Decision process; this is an Under Secretary driven supra process.

- Performance Measurement & Reporting – this process provides the direction for effectively measuring the success of the policies, guidance, bulletins, Program Cyber Security Plans (PCSPs), System Security Plans (SSPs), Standard Operating Procedures (SOPs, and other related documentation.

4.3 Program Components

As Figure 3 indicates, the cyber security program is composed of several components, including planning, policy, management and technology, services, and performance management. Each of these components will be described in greater detail in later sections of this plan. However, it is the mutually reinforcing nature of these elements of cyber security, which emphasize the need for a strong governance structure for the cyber security program; a structure that allows senior leadership to see across the program and coordinate with each other across the Department; places responsibility and accountability at appropriate levels; and sets, measures, and rewards performance.

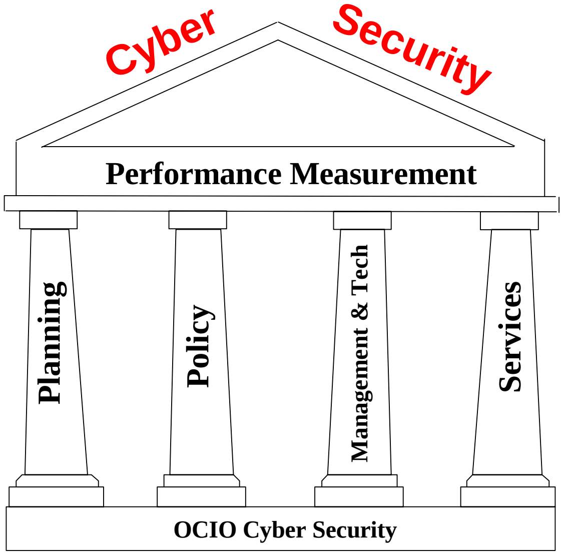


Figure 3. Cyber Security Program Components

4.3.1 Cyber Security Planning

The OCIO is responsible for identifying overall cyber security goals and outcomes for DOE. The OCIO is also responsible for the development, implementation, and ongoing management of all information systems security and controls necessary to safeguard assets, ensure data integrity and confidentiality, support business continuity, and ensure compliance with all regulations and best practices. With the assistance of the ESC and its supporting CSWG, the OCIO employs a risk management based program, identifies regulatory requirements, develops and implements effective policies, guidance and procedures, and ongoing maintenance of cyber security control mechanisms. In order to accomplish these goals security-planning activities must take place. Planning is supported by a collaborative effort to understand the threat landscape and identify weaknesses through reviews and performance measurement. This information is fed back into the planning activities to generate both a long-term strategic plan and an annual tactical plan. These plans are then communicated in a top down approach to all the stakeholders for implementation.

The following set of sub processes, which fall within the Leadership Decision supra process, address the planning component.

- Departmental Cyber Security Strategic Planning – this sub process establishes the desired outcome of and the necessary steps toward the effective creation of the DOE strategic plan.

- Departmental Cyber Security Tactical Planning – this sub process establishes the desired outcome of and the necessary steps toward the effective creation of an annual tactical plan. It identifies the near-term goals of the Department and prioritizes them by importance to enhancing the security posture, and it then establishes a template for creating a plan that addresses those goals.

- Departmental Threat Statement Development – this sub process documents the standard approach for developing a Departmental threat statement.

- Departmental Risk Assessment Development – this sub process documents a standard approach to developing the Department's risk assessment.

4.3.2 Cyber Security Policy

The policy component is very closely aligned with both the governance program and the planning component. Cyber Security Policies establish the high-level goals and outcomes for the overall DOE Cyber Security Program. Enhanced through guidance, and performance metrics, the Policy is in place to drive the program's implementation. The focus is on top-level policy supported by guidance at the Departmental Level. It is the responsibility of the Under Secretary and staff office elements to implement it.

To ensure the best possible results and to ensure that a standard approach across the Department is achieved, the following sub process, which falls within the Leadership Decision supra process, addresses the policy component.

- Policy and Guidance Development Process – outlines the various mechanisms in place for approving policy. It details the various pros and cons of each mechanism and provides advice on which mechanism is most applicable for various policy documents.
    - Directives System – documents the process and provides the steps necessary to submit policy via this decision process.
    - Guidance – outlines the process by which new concepts for guidance are introduced to the CSWG for acceptance.
    - Bulletins – provides the steps to create a bulletin for Departmental distribution by the OCIO.

4.3.3 Cyber Security Management & Technology

The keystone to a successful security program is a well-maintained and documented technology management plan that clearly defines the purpose, scope, and usage of technology. This baseline leads to the successful implementation of security controls throughout the architecture. Given its federated structure, the Department of Energy operates a diverse, geographically separate, inter-connected group of computing enclaves, each of which is locally managed and secured, and most of which house multiple systems. Due to this model, it becomes apparent that without clear direction, the Department is susceptible to lapses in security at various points of the architecture.

Installing well-defined, high-level Department structure, processes, and principles puts the Department in position to successfully manage the technology it employs. Identifying and establishing key targets areas asset management, certification and accreditation, and cyber security technology allows targeted efforts to create lasting directives for handling accountability, authorized system operation, and approved security solutions.

To achieve the best possible results from this structure and to ensure that a standard approach across the Department is achieved, the following set of sub processes, which fall within the Leadership Decision supra process, address the management and technology component.

- Architectural Guidance – creates the definition of the standard Department technology architecture and provides the process by which new technologies are reviewed for acceptance into the guidance
- Enterprise Licensing – provides a process that incorporates the needs of the entire Department when considering enterprise application licensing.
- Technology Review – documents a standardized approach to the review of new technologies that may be of interest to the Department. This sub process may directly tie to enterprise licensing.
- Technology Development – documents the process of initiating the development/introduction of a new system or technology that may be beneficial to the entire Department.

4.3.4 Cyber Security Services

Sizeable changes to any organization can be difficult. As Under Secretary and Program Offices adapt to the new processes and policies, it is the role of the OCIO to help make that adjustment thorough various services and through performing several key initiatives that protect the entire Department. This is accomplished through a revised management approach that involves the entire Department. The revised management approach focuses on empowering the Under Secretary and Program Offices.

The role of the OCIO in the new approach involves providing program oversight and high-level policy recommendations. The OCIO will lead in developing guidance, bulletins, and metrics that will be implemented throughout the Department. The Deputy Secretary will approve these policies and the OCIO will provide compliance monitoring and reporting on their implementation and effectiveness.

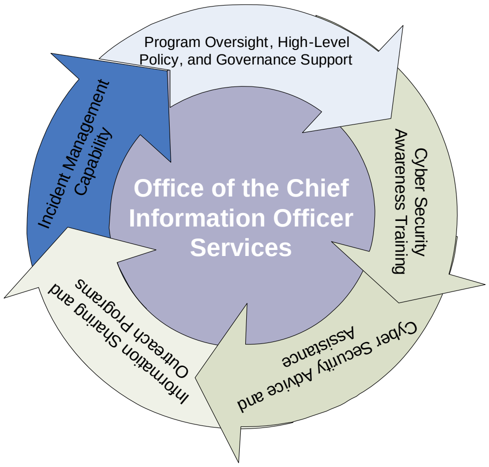

Program Oversight, High-Level Policy, and Governance Support
Cyber Security Awareness Training
Cyber Security Advice and Assistance
Information Sharing and Outreach Programs
Incident Management Capability
Office of the Chief Information Officer Services

Figure 4. CIO Services

Although the Under Secretary and Program Offices are charged with more responsibilities, the OCIO is expanding its role to assist and help with these changes. The OCIO will continue to be the point at which high-level policy is determined, but these policy decisions are made through the support of subordinate organizations that provide input via the ESC, and the CSWG. In addition to governance support, the OCIO will ensure that Department's management understands the threats to the organization and their roles through establishing cyber security awareness training and role-based training.

Several programs will focus on outreach, information sharing, and advice and assistance. The aim of these programs is to develop an intelligent, proactive approach to mitigating the security threat to the Department and other Agencies. This is accomplished through sharing incident data with other Agencies and ensuring that the Department is kept abreast of developing threats across the Department. If advice and assistance is required by any part of the Department, the OCIO is available to assist in a variety of activities, such as risk mitigation or incident recovery.

To deliver the best possible results from these services and to ensure that a standard approach to delivery is achieved, the following set of sub processes, falling under the Leadership Decision supra process, address the services component.

- Cyber Security Communications – assures a clear process for the dissemination of cyber security threat and incident information with Departmental and Other Agencies.
- Cyber Security Education and Awareness – establishes a process for Departmental cyber security awareness and education.
- Asset and Inventory Management – installs a mechanism by which Departmental organizations can report inventory and request automated asset management functions.
- Certification and Accreditation Assistance – demonstrates the means by which Departmental organizations can request assistance for Certification and Accreditation activities.
- Cyber Security Advice and Assistance – creates a process by which Departmental organizations can receive cyber security support from the OCIO.
- Awards and Recognition – documents the criteria and process for being recognized as a cyber security practice leader within the DOE.

4.3.5 Cyber Security Performance Measurement

Performance measurement, Figure 5, provides a clear and consistent way to measure success and demonstrate results for senior management. It helps to maintain a high-level overview of the current security posture by defining repeatable metrics and critical success factors. It ensures legislative, policy, and guidance requirements are being met. It further identifies functional and organizational gaps that could impede the cyber security program's success. Finally, it provides feedback mechanism to adjust cyber security program and implementation, as needed.

To capture the best practices and lessons learned of the cyber security program and to ensure that a standard approach to measurement of success factors is achieved, the following performance measurement processes and its supporting sub processes address the performance measurement component.

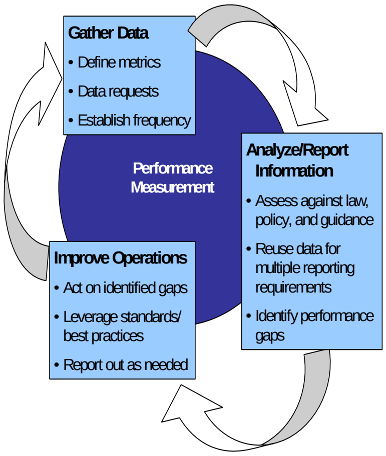

Gather Data
• Define metrics
• Data requests
• Establish frequency
Performance Measurement
Analyze/Report Information
• Assess against law, policy, and guidance
• Reuse data for multiple reporting requirements
• Identify performance gaps
Improve Operations
• Act on identified gaps
• Leverage standards/ best practices
• Report out as needed

Figure 5. Performance Measurement

- Performance Measurement – details the Department's definition of success and the required steps to meet the expectation.
  - Metrics Development – ensures that a process for developing the criteria by which the Department can effectively evaluate implementation based on a common set of baseline measurements.
  - Compliance and Monitoring Reviews – documents the process followed to ensure compliance with established policy and guidance.
  - Compliance Reporting – establishes the process of delivering a standard set of reports that documents the Departments current cyber security posture and FISMA milestones.
  - Maturity Measurement – a process that incorporates the results from all the defined performance measurement processes and compares them to an earlier state to determine the maturity of the program.

4.4 The OCIO Role

With the OCIO assuming an oversight position in the new management approach, the Under Secretary and Program Offices take a more active role in the security of their organizations. They will oversee all the planning and requirements development necessary that lead to program implementation. Although each is empowered to make the necessary decisions for their various organizations, they must implement their program in such a way that is consistent with Department policy and guidance.

The Under Secretary and Program Offices will assume responsibility for their own Cyber Security Program Plans. This change recognizes the Under Secretaries as key players in cyber security implementation across the Department. It also provides a link between OCIO policy and guidance and the actual Under Secretary implementation. This ensures a consistency between DOE cyber security policies, guidance, bulletins, and metrics, while still allowing organizational policy to be adapted based on mission and culture. This change is a revision and builds on already established cyber security planning that is happening at the organizational level.

While the challenge is great, it is achievable. The objectives laid out in the following sections will provide the details to move the revitalization of the DOE security posture forward into the next generation. This is just the roadmap that directs the activities that need to take place, but there is a need to apply the necessary resources to accomplish the objectives set forth. There is a strong desire to leverage the existing capabilities that have been developed and ensure that solutions meet the needs of the Department's varied missions.

5. Cyber Security Program Roadmap

Figure 6 provides a visual representation of the program's components and their associated activities. The figure depicts the efforts already underway to address the immediate and short-term remediations recommended by the Cyber Security Project Team (CSPT) and the DOE OCIO, and the long-term strategy to improve the Department's cyber security program. Only the major OCIO milestones for the next twelve months are shown, continuous improvement of the DOE Cyber Security Program will occur throughout the entire program. The figure provides a high-level understanding of the critical activities supporting the revitalized program and the approximate point in time over the next 12-month period when the activities will be available for Under Secretary implementation[1].

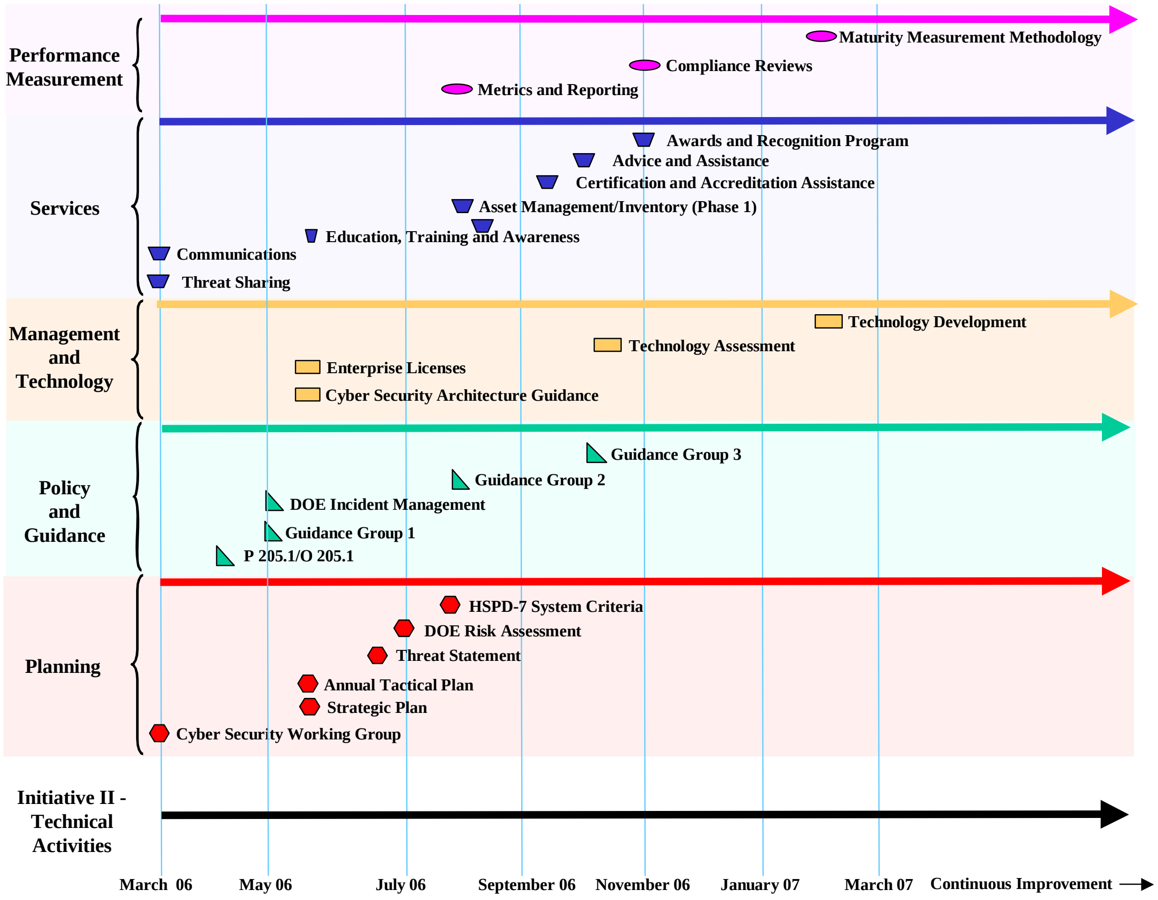


Figure 6. Revitalized Cyber Security Program Roadmap

Table 1 below expands on the information conveyed in the above char, providing basic descriptions for the cyber security program activities, grouped by program component, and with associated estimated time to complete.

Table 1. Cyber Security Program Component to Activity Table

Cyber Security Program Component	Cyber Security Program Activity		Cyber Security Program Activity Number	Estimated Development Duration
Cyber Security Planning	Annual Tactical Plan		5.1.1	2 - 4 months
	Department Cyber Security Risk Assessment		5.1.2	2 months
	Strategic Plan		5.1.3	2 - 3 months
	Threat Statement		5.1.4	3 - 4 months
Cyber Security Policy and Guidelines	DOE P 205.1 / O 205.1		5.2.1	2 months
	Guidance	Certification and Accreditation	5.2.2	2 months
		Clearing and Sanitization	5.2.3	3 - 6 months
		Compliance Reviews	5.2.13	1 - 2 months
		Configuration Management	5.2.4	3 - 6 months
		Contingency Planning	5.2.6	3 - 6 months
		Controls	5.2.7	1 - 2 months
		Foreign National Access	5.2.8	3 - 6 months
		HSPD-7	5.2.9	3 - 4 months
		Incident Management	5.2.10	1 - 2 months
		INFOCON	5.2.11	3 – 6 months
		Interconnection Agreements	5.2.12	1 - 2 months
		IPv6 Network and Security Planning	5.2.13	3 - 6 months
		National Security	5.2.13	3 - 6 months
		Password Management	5.2.15	1 - 2 months
		Peer-to-Peer	5.2.16	3 - 6 months
		Personally Owned Computing	5.2.17	3 - 6 months
		Plan Of Action & Milestones (POA&M)	5.2.18	3 - 6 months
		Portable/Mobile Computing	5.2.19	3 - 6 months
		Remote Access to DOE Information Systems	5.2.20	3 - 6 months
		Risk Management	5.2.21	1 - 2 months
		Vulnerability Scanning	5.2.22	1 - 2 months
		Voice Over Internet Protocol	5.2.23	3 – 6 months
		Wireless Devices and Information Systems	5.2.24	3 - 6 months

[1] The Policy and Guidance section of the figure arranges the guidance documents to be developed under this plan into three groups. The guidance in each group is determined by the priority of need across the Department. Group 1 is expected to contain Controls, Risk Management, Vulnerability Scanning, Certification and Accreditation, Incident Management, Interconnection Agreements, and Compliance Reviews. Group 2 is expected to contain Contingency Planning, Configuration Management, Clearing and Sanitization, Password Management, Wireless Devices and Information Systems, Portable/Mobile Computing, Remote Access to DOE Information Systems, and Foreign National Access. Group 3 is expected to contain POA&M, Peer-to-Peer, Personally Owned Computing, HSPD-7, Ipv6, and Voice Over IP.

Cyber Security Program Component	Cyber Security Program Activity	Cyber Security Program Activity Number	Estimated Development Duration
Cyber Security Architecture & Technology Management	Cyber Security Architecture Guidance	5.3.1	2 - 4 months
	Defensive Response	5.3.2	3 – 6 months
	Enterprise Licenses	5.3.2	1 - 4 months
	Technology Assessment	5.3.4	2 - 8 months
	Technology Development	5.3.5	3 - 14 months
Cyber Security Services	Advice and Assistance	5.4.1	1 - 6 months
	Asset and Inventory Management	5.4.2	1 – 12 months
	Automated “OPSEC” Analysis of Web Sites and Servers	5.4.3	6 – 12 months
	Awards and Recognition Program	5.4.4	2 - 4 months
	Certification and Accreditation Assistance	5.4.5	1 - 7 months
	Cyber Security Working Group	5.4.7	Underway
	Communications (internal and external)	5.4.7	Underway
	Education, Awareness, and Training	5.4.8	1 - 3 months
	DOE Incident Management	5.4.10	1 - 3 months
	Threat Sharing	5.4.9	Underway
	Network Infrastructure Mapping	5.4.11	Underway
Cyber Security Performance Measurement	Maturity Measurement Methodology	5.5.1	4 - 8 months
	Metrics and Reporting	5.5.2	3 - 6 months
	Compliance Reviews	5.2.4	3 - 7 months

5.1 Cyber Security Planning Activities

5.1.1 Annual Tactical Plan

This activity is the development and implementation of the annual action plan for the cyber security activities in the DOE Chief Information Officer organization. The annual action plan includes the DOE cyber security-related activities identified in this revitalization plan and the cyber security activities within the DOE OCIO organization. The action plan includes milestones and deliverables for each of the activities in the plan and is used to guide the cyber security efforts in the DOE OCIO organization for the entire year covered by the plan.

Deliverable:

- Annual DOE OCIO cyber security action plan, approved by the DOE OCIO.

5.1.2 DOE Risk Assessment

The Department Risk Assessment will provide a baseline understanding of the risk environment associated with DOE’s varied missions and assets. This assessment will be based on established federal standards and geared toward providing a foundation upon which the Under Secretary organizations can build customized risk assessments for their security programs and subordinate elements. The risk assessment will proactively provide senior leadership a clearer understanding of the magnitude and severity of threats facing the Department as well as the potential vulnerabilities those threats would seek to exploit.

Deliverable:

- Departmental Risk Assessment coordinated with the ESC and approved by the DOE OCIO.

5.1.3 Cyber Security Strategic Plan

The Cyber Security Strategic Plan is intended to chart the future of the DOE cyber security program and ensure that the program is better prepared to meet the Department's cyber security requirements. The plan details how the program intends to counter the evolving threat with improved protection capabilities. The plan describes how we will strive to achieve better efficiency and effectiveness in the cyber security program. This plan is designed with a timeframe of only ten years; however, it is conceivable and indeed, quite likely, that many of the objectives and strategies posited in this plan will be germane and/or in implementation many years from now.

Deliverables:

- Process for developing and maintaining a DOE Cyber Security Strategic Plan benchmarked against other government and private organizations.
- Process for regular coordination of cyber security strategic plan with DOE stakeholders.
- 2006-2007 DOE Cyber Security Strategic Plan.
- ESC approval of the initial cyber security strategic plan.

5.1.4 Threat Statement

This document provides an assessment of cyber threats to information and information systems in the DOE. Threat is defined as anything initiated by a perpetrator that can affect the confidentiality, integrity, or availability of an information system and its data. This statement considers threats to DOE information and information systems as well as those critical infrastructures owned by DOE or those for which DOE is the relevant U.S. government agency. The threat statement is based on, and incorporates, the threats and threat levels in the "Cyber Threat to the United States" and "The Foreign Cyber Threat to the United States Department of Energy (Draft)" documents. The threat statement is also based on cyber threat guidance developed by the U.S. Government Intelligence Community and the Department of Energy intelligence organizations.

Deliverable:

- Updated DOE Cyber Threat Statement

5.2 Cyber Security Policy and Guidelines

5.2.1 DOE P 205.1 / DOE O 205.1-1

DOE P 205.1, *Departmental Cyber Security Management Policy*, describes the policy components that make up the management of cyber security within the Department. DOE O 205.1-1, *Department Of Energy Cyber Security Management Program Objectives*, replaces the current DOE O 205.1 and provides information security protections consistent with DOE P 205.1 that are commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of DOE. The program defined in this policy will implement the requirements of applicable Federal laws and regulations using a mission-compatible, cost-effective risk management process that applies appropriate measures to ensure the confidentiality, integrity, and availability of cyber information and information systems. This policy establishes a federated Program that integrates cyber security governance, accountability, and reporting into management and work practices across the Department. This policy includes the responsibility for line managers to make cyber security risk management decisions, including responsibilities for formally accepting residual risk.

A section in DOE O 205.1-1, or possibly a new DOE M 205.1, *National Security Information Systems Security Manual*, will replace the current DOE M 471.2-2, *Classified Information Systems Security Manual* and provide national security information protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of DOE. The requirements defined in this order will implement the requirements of applicable Federal laws and regulations using a mission-compatible, cost-effective risk management process that applies appropriate measures to ensure the confidentiality, integrity, and availability of national security systems and information.

This order will include a requirement for each Under Secretary to improve accountability for contractor performance by increasing award fees for cyber security to levels commensurate with those for other support functions (e.g., safety, physical security)

Deliverable:

- Revised DOE O 205.1-1 {in development}

5.2.2 Certification and Accreditation Guidance

This guidance establishes the minimum requirements for the certification and accreditation of all DOE information systems. This guidance will cancel DOE N 205.9, *Certification and Accreditation Process for Information Systems Including National Security Systems*.

Deliverable:

- DOE Guidance on certification and accreditation of information systems. {In development}

5.2.3 Clearing and Sanitization Guidance

This guidance establishes the minimum requirements for clearing, sanitizing, and destroying DOE information system storage media, memory devices, and related hardware. This guidance will cancel DOE M 205.1-2, *Clearing, Sanitization, And Destruction Of Information System Storage Media, Memory Devices, And Related Hardware Manual*.

Deliverable:

- DOE Guidance on the clearing, sanitization and destruction of media and devices.

5.2.4 Compliance Reviews Guidance

This guidance establishes the processes and criteria for conducting compliance reviews of the cyber security program by the DOE Chief Information Officer organization. The compliance review will evaluate a PCSP using DOE cyber security policy and guidance issued by the DOE OCIO. Results from the compliance review will be provided to the Under Secretary for use in improving the Under Secretary's cyber security program documented in the PCSP. The review will evaluate selected site implementation of the PCSP being reviewed. Selected information systems at the site may be reviewed to validate the site's implementation of the Under Secretary PCSP and the site's cyber security program. Results from the monitoring review will be provided to the site and the Under Secretary for use in improving the implementation of the site's cyber security program and improving the Under Secretary PCSP. Results from the compliance reviews will be used by the DOE OCIO to improve the DOE cyber security program.

To minimize the impact of compliance reviews on the sites, the OCIO will coordinate with the IG and the Office of Independent Oversight and Performance Assessment to reduce, and eliminate where possible, any duplication of efforts.

Deliverable:

- DOE Guidance on conducting cyber security compliance and monitoring reviews.

5.2.5 Configuration Management Guidance

This guidance establishes the minimum requirements for configuration management of all DOE information systems, including recommendations for secure system configuration specifications.

Deliverable:

- DOE Guidance on configuration management of DOE information systems.

5.2.6 Contingency Planning Guidance

This guidance establishes the minimum requirements for contingency planning for all information systems within DOE. The guidance establishes a graded approach to contingency planning and testing.

Deliverable:

- DOE Guidance on contingency planning for all DOE information systems.

5.2.7 Controls Guidance

This DOE OCIO Guidance specifies the DOE cyber security program requirements and provides minimum guidance for implementing NIST 800-53 management, operations, and technical controls for information systems within the DOE, including the NNSA. It incorporates the requirements of Public Laws, Federal Regulations, and Departmental regulations.

This guidance also lists cyber security responsibilities for all critical positions impacting cyber security within DOE and contractor organizations.

Deliverable:

- DOE Guidance on application of NIST 800-53 controls to Under Secretary and Staff Office PCSPs.

5.2.8 Foreign National Access Guidance

This guidance establishes the minimum requirements for foreign national access to DOE information systems. This guidance also lists cyber security roles and responsibilities for all positions involved with foreign national access to DOE information systems within DOE and contractor organizations. This guidance will cancel DOE N 205.2, *Foreign National Access To Doe Cyber Systems.*

Deliverable:

- DOE Guidance on foreign national access to DOE information systems.

5.2.9 Homeland Security Presidential Directive (HSPD)-7 Guidance

This guidance establishes the minimum requirements and process for identifying, managing, and protecting critical infrastructure and key resources related to or associated with

DOE information systems consistent with HSPD-7 and with the identification of Primary National and Mission Essential Functions (per White House January tasking).

Deliverables:

- DOE Guidance for the identification, managing, and protecting critical infrastructure and key resources in accordance with DOE's response to HSPD-7 and with the identification of Primary National and Mission Essential Functions (per White House January tasking).

5.2.10 Incident Management Guidance

Review the Department's cyber security incident warning, prevention, detection, and response processes. Cyber security incident management responsibilities and authorities need to be assessed for clarity across the Department and for coordinated approaches for responding to varying incident conditions.

This guidance establishes the minimum requirements for a structured, cohesive, and consistent process for performing incident warning, response, and management (sometimes referred to collectively as incident management) for DOE information systems. This guidance will cancel DOE M 205.1-1, *Incident Prevention, Warning, And Response (IPWAR) Manual*.

Deliverables:

- DOE guidance on cyber incident warning, prevention, detection, response, and management across the Department.

5.2.11 Information Condition (INFOCON) Guidance

The DOE INFOCON system defines actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks (CNA), and to mitigate sustained damage to DOE information and infrastructure, including computer and telecommunications networks and systems. The INFOCON is a comprehensive defense posture and response based on the status of information systems, DOE and program office operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system impacts all personnel who use DOE information systems, protects systems while supporting mission accomplishment, and coordinates the overall defensive effort through adherence to guidance.

INFOCON also outlines countermeasures to scanning, probing, and other suspicious activity, unauthorized access, and data browsing. DOE INFOCON measures will focus on computer network-based protective measures, due to the unique nature of CNA. CNA is defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Each level reflects a defensive posture based on the risk of impact to DOE and program office operations through the intentional disruption of information systems and networks.

INFOCON levels are NORMAL (normal activity), ALPHA (increased risk of attack), BRAVO (specific risk of attack), CHARLIE (limited attack), and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions.

Implementing a DOE INFOCON will require developing the appropriate polices defining the roles, responsibilities, and expected actions at each of the INFOCON levels. Implementation will also require developing a separate secure capability to communicate with the cyber security personnel at each of the DOE offices and sites.

Interaction with the intelligence community regarding indicators of possible attacks and resolution of identified attack activities well is necessary to initiate or change an INFOCON level.

Deliverables:

- DOE guidance on the definition, implementation, and operation of a Department-wide INFOCON process.

5.2.12 Interconnection Agreements Guidance

This guidance establishes the minimum requirements for the authorization of all connections from outside of the accreditation boundary of an information system to other information systems and monitoring/controlling the system interconnections on an ongoing basis.

Deliverable:

- DOE Guidance on Interconnection Agreements.

5.2.13 IPv6 Network and Security Planning Guidance

This guidance established the minimum requirements for the design and planning associated with transitioning the Department to the IPv6 standard.

Deliverable:

- DOE guidance on the planning for IPv6.

5.2.14 National Security Guidance

This guidance defines a graded, risk-management management, operations, and technical controls for protecting classified data and national security information systems in the Department.

Deliverable:

- DOE guidance on protection measures for national security information systems.

5.2.15 Password Management Guidance

This guidance establishes minimum requirements for the generation, protection, use, and distribution of passwords to support authentication when accessing classified and unclassified DOE information systems. This guidance will cancel DOE N 205.3, *Password Generation, Protection, And Use* and DOE G 205.3**,** *Password Guide***.**

Deliverable:

- DOE Guidance on Password Management.

5.2.16 Peer-to-Peer Technology Guidance

Peer-to-peer (P2P) technology refers to any software or system that allows individual users of the Internet to connect (directly, through the Internet) to each other to transfer or exchange computer files. The definition used by the Federal Enterprise Architecture is that P2P technology is a class of applications that operates outside the Internet Domain Name Service (DNS) system, that has significant or total autonomy from central servers, and that takes advantage of resources available on the Internet.

Federal computer systems or networks (including those operated by contractors on behalf of Commerce) must not be used for downloading illegal and/or unauthorized copyrighted content in accordance with Office of Management and Budget Memorandum 04-26, *Personal Use Policies and File Sharing Technology*. DOE prohibits unauthorized P2P file sharing technology from use on DOE information systems unless it has been explicitly authorized in writing by an operating unit OCIO in support of an official application. Special attention to ensuring that public P2P technology is not being used to support sharing of computer files that contain music, digital film, TV shows or other information such that copying of the files may infringe on any copyrights or other associated intellectual property restrictions. For the purposes of this policy, collaborative research and computing technologies such as Grid computing (e.g., Globus) are specifically excluded from the definition of P2P technology; as long as the content of internode communication remains free of copyrighted material.

Deliverable:

- DOE Guidance on the use of Peer-to-Peer Technology.

5.2.17 Personally Owned Computing Guidance

This guidance establishes the minimum requirements for the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information. Operating units may develop policies covering use of personally owned computing resources beyond the requirements in this guidance, but such policies must be consistent with this guidance.

Deliverable:

- DOE Guidance on the use of personally owned computing technology.

5.2.18 Plan Of Action & Milestones Guidance

A plan of action and milestones (POAM) documents the operating unit's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system.

This guidance provides the minimum requirements for development and management of POA&Ms to track corrective actions when external audits, reviews, or self-assessments reveal deficiencies in a DOE information system. This guidance also describes the requirements for the consistent and comprehensive completion of required updates of information system POA&Ms and establishes reporting schedules and formats for POA&Ms.

Deliverable:

- DOE Guidance on development and management of POA&Ms.

5.2.19 Portable / Mobile Computing Guidance

This guidance establishes the minimum requirements for the use of portable/mobile devices and information systems within DOE. Operating units may develop policies covering use of portable/mobile computing resources beyond the requirements in this guidance, but such policies must be consistent with this guidance.

Deliverable:

- DOE Guidance on the use of portable/mobile computing technology.

5.2.20 Remote Access to DOE Information Systems Guidance

This guidance establishes the minimum requirements for remote connection to DOE information systems. This guidance will cancel DOE N 205.11, *Security Requirements For Remote Access To DOE And Applicable Contractor Information Technology Systems.*

Deliverable:

- DOE Guidance on Remote Access to DOE and DOE-Contractor Systems.

5.2.21 Risk Management Guidance

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guidance provides a foundation for developing an effective risk management program, containing both the definitions and the practical direction necessary for assessing and mitigating risks identified to DOE information and information systems. This guidance will enable management to make well-informed risk management decisions to justify the expenditures that are part of capital planning and budget and assist management in authorizing (or accrediting) DOE information systems on the basis of the supporting documentation resulting from the performance of risk management. The guidance describes the DOE requirements for implementing a risk management approach for all information systems within DOE.

Deliverable:

- DOE Guidance on Risk Management {in development}.

5.2.22 Vulnerability Scanning Guidance

This guidance establishes the minimum requirements for using appropriate vulnerability scanning tools and techniques to scan for vulnerabilities in the information system routinely or when significant new vulnerabilities affecting systems are identified and reported.

Deliverable:

- DOE Guidance on vulnerability scanning of DOE information systems.

5.2.23 Voice Over Internet Protocol Guidance

Protective measures consistent with the recommendations in National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems,* graded according to system sensitivity are needed to ensure proper use of voice over IP (VOIP) technology. Different from traditional circuit-based telephony, voice over IP technology permits voice transmission over packet-switched IP networks. VOIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units, and mobile units, and may include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Because of the time-critical nature of VOIP, and its low tolerance for disruption and packet loss, many security measures implemented in traditional data networks are simply not applicable to VOIP in their current form; firewalls, intrusion detection systems, and other components must be specialized for VOIP.

Deliverable:

- DOE Guidance on the use of technologies employing VOIP technologies.

5.2.24 Wireless Devices and Information Systems Guidance

This guidance establishes DOE minimum requirements for using wireless devices and information systems within DOE. This guidance will cancel DOE N 205.8, *Cyber Security Requirements for Wireless Devices and Information Systems.*

Deliverable:

- DOE Guidance on the use of Wireless Devices and Information Systems.

5.3 Cyber Security Architecture and Technology

5.3.1 Cyber Security Architecture Guidance

The DOE enterprise architecture must include developing a comprehensive architecture for the Department's cyber security activities by clearly defining the business activities and the roles and responsibilities for carrying them out. The architecture will be driven by the Department's strategies and will tie cyber security management business activities to those strategies, with specific performance metrics defined to ensure that the architecture results in measurable benefits to the Department. The enterprise architecture should also address HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, and HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. This guidance will cancel DOE G 205.1, *Cyber Security Architecture Standards*.

Deliverables:

- DOE cyber security architecture guidance.

5.3.2 Defensive Response

Current tools to react when internal or external malicious activity is suspected currently do not exist or are extremely immature. It should be possible to track an attacker's activities carefully, thoroughly, and inconspicuously, as a reaction to indicators of suspicious activity.

Reaction tools are needed to aid system administrators and security personnel to quickly assess potential problems, apply tracking and surveillance tools, and conduct damage control as necessary, etc. If warning signs are unclear or ambiguous, it may be necessary to track a user's activities surreptitiously for an extended period. These tools must be usable by system administrators without requiring extensive training and expertise.

A robust and flexible adaptive defense capability requires the following characteristics. The adaptive defense capability is needed in the unclassified and national security computing systems and networks in all DOE sites and in the DOE enterprise.

- Reaction management systems capable of 1) creating traffic among sets of information systems to covertly degrade malicious activity; 2) adapting to changes in network topologies and conditions to control information flows within the network and enterprise; and 3) analyzing coordinated timing data for information flows at various nodes within a network and across the enterprise.
- Deception management systems capable of 1) assuming control of ongoing communication sessions in a manner that avoids noticeable alterations in system behavior; 2) simulating the network environment in which the normal system operates to convince an attacker that the simulated environment is the real one; and 3) replacing internal services on the fly without noticeable impact on user behavior or performance.
- Analysis and response management systems capable of 1) gathering, integrating, and analyzing data received from distributed intrusion detection systems in the network and enterprise; 2) controlling reaction and deception systems to mitigate consequences of an attack while avoiding detection by the attacker; and 3) analyzing current and future situations to anticipate the need for action and pre-positioning of capabilities allowing rapid reaction to future events.
- Real-time and post mortem forensic systems capable of: 1) gathering and storing historical and real-time information from all available data sources, and integrating the information to allow for analysis of events over time and system type; 2) generating paths of entry and location of sources and intermediaries used by the attacker, based on the available audit information; and 3) correlating and analyzing information from diverse sources of audit and intrusion data that may be partially redundant.

Retaliation is an important part of an adaptive defense capability, but careful consideration must be given to all aspects of any retaliation capability. Significant legal issues must be addressed when considering a retaliation capability. U.S. government organizations are prohibited from conducting some retaliation activities that may be allowed for private entities, such as, contractors. Retaliation, or response options include, but are not limited to, terminating the offending connection, blocking the source IP address of the offending packet(s), managing traffic flows (see above), and/or attack analysis. Although the response could be automated, great care must be taken to prevent service disruption of critical site and enterprise resources from false positives or denial of service scenarios. Resolution of the legal issues is necessary before developing any retaliation capability in the DOE.

Deliverables:

- o Reaction management systems deployable at each site, integrated across the Department, and capable of 1) creating traffic among sets of information systems in order to covertly degrade malicious activity; 2) adapting to changes in network topologies and conditions to control information flows within the network and enterprise; and 3) analyzing coordinated timing data for information flows at various nodes within a network and across the enterprise.

- Deception management systems deployable at each site, integrated across the Department, and capable of 1) assuming control of ongoing communication sessions in a manner that avoids noticeable alterations in system behavior; 2) simulating the network environment in which the normal system operates, in order to convince an attacker that the simulated environment is the real one; and 3) replacing internal services on the fly without noticeable impact on user behavior or performance.
- Analysis and response management systems deployable at each site, integrated across the Department, and capable of 1) gathering, integrating, and analyzing data received from distributed intrusion detection systems in the network and enterprise; 2) controlling reaction and deception systems to mitigate consequences of an attack while avoiding detection by the attacker; and 3) analyzing current and future situations in order to anticipate the need for action and pre-positioning of capabilities allowing rapid reaction to future events.
- Real-time and post mortem forensic systems deployable at each site, integrated across the Department, and capable of 1) gathering and storing historical and real-time information from all available data sources, and integrating the information to allow for analysis of events over time and system type; 2) generating paths of entry and location of sources and intermediaries used by the attacker, based on the available audit information; and 3) correlating and analyzing information from diverse sources of audit and intrusion data that may be partially redundant.

5.3.3 Enterprise Licenses

Establish cost-efficient procurement vehicles for acquiring cyber security tools, services, and solutions. Sites need to have cost-efficient procurement vehicles in place to facilitate obtaining tools and operating systems that will support such cyber security needs as asset management, configuration management, minimum security configuration guidance, vulnerability management, and intrusion detection.

Deliverables:

- Acquisition of enterprise licenses for tools to implement cyber security controls at DOE sites.

5.3.4 Technology Assessment

Technology assessment activities in the DOE Cyber Security Program must include three distinct, but overlapping, activities. One set of activities should be focused on developing and maintaining an awareness of the technologies being developed in the DOE laboratories and production facilities. These technologies may be developed for other sponsors or for in-house use, and this effort should evaluate the technologies for possible use in the DOE cyber security program. This activity would provide the leadership to adapt the technologies for use in the DOE program.

Another set of activities should be focused on developing and maintaining an awareness of the technologies being developed in other government agencies and their contractors. These technologies may be developed for other sponsors or for in-house use and this effort should evaluate the technologies for possible use in the DOE cyber security program. This activity would provide the leadership to adapt the technologies from other agencies for use in the DOE program.

A third set of activities involves a proactive approach to identifying emerging information and information assurance technologies and products. Assessments of these emerging products are required to develop a comprehensive awareness of the:

- Inherent vulnerabilities and weaknesses of current and future technologies that may be used in DOE information systems and networks;
- Technologies that potentially could be used to disrupt, damage, or destroy data or components; and
- Impact on the DOE information protection threat assessment, policies and practices; and potential uses in the DOE mission activities.

Deliverables:

- Processes to develop and maintain awareness of technology development activities in DOE laboratories, production facilities, other government agencies, and vendors;
- Annual report to DOE OCIO and ESC on technology assessment activities.

5.3.5 Technology Development

Within the constraints of the priorities of the DOE cyber security program and available funding, DOE must undertake to augment the availability of commercial cyber security tools and solution to address requirements unique to DOE because of the diverse missions, the geographically distributed sites, the high degree of interconnectivity among the sites, and the need to employ advanced information technologies throughout the Department. This augmentation will include a mix of sponsoring the prototyping of tools identified in the Technology Assessment, section 5.3.4, activities, as well as developing and deploying specific tools to meet Department’s needs. DOE development should be initiated only upon confirming that no commercial or other government-sponsored effort can be adapted to meet DOE’s needs.

Deliverable:

- Process to develop and maintain an annual DOE cyber security technology development program, including funding requirements.
- Annual report to DOE OCIO and ESC on technology development activities.

5.4 Cyber Security Services

5.4.1 Advice and Assistance

Establish an advice and assistance function to support line management implementation of cyber security requirements. This function would provide support and assistance to line management and contractor organization in implementing cyber security requirements consistent with DOE objectives and expectations.

Deliverables:

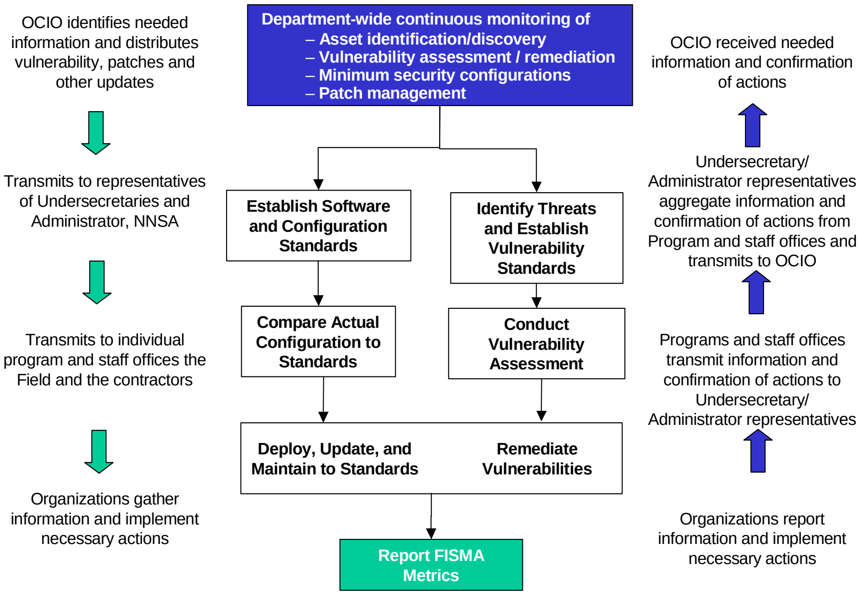
- Definition of a process for requesting advice and assistance.
- Identifying, and making available, cyber security subject matter experts within the Department to assist line management and contractor organizations with technical or programmatic issue compliance in accordance with Departmental policies, guidance, and bulletins.
- Identifying, and making available, cyber security subject matter experts within the Department to assist line management and contractor organizations in reviewing, correcting existing, and creating new policies and procedures to provide evidence of compliance with Departmental policies, guidance, and bulletins.
- Identifying, and making available, cyber security subject matter experts within the Department to conduct training workshops and explain DOE policies to line management and contractor organizations to facilitate consistent implementation of security controls as well as improved security budget requests.
- Identifying, and making available, cyber security subject matter experts within the Department to provide advice and assistance in applying and implementing technical tools for enhancing cyber security.
- Communicating the advice and assistance program across the Department.

5.4.2 Asset Management/Inventory

The DOE Continuous Asset Monitoring System (CAMS) capability provides a Department-wide framework for operating and developing existing and future asset management systems. The DOE CAMS is generic and flexible, able to adapt to changing technologies while continuing to address DOE asset management requirements in ever more sophisticated and convenient ways.

CAMS is focused on the information systems, including desktops; workstations; servers; network components, such as routers; security devices, such as firewalls, access controls, and user authentication; printers; wireless access systems; mid-range computing resources; mainframe computers; process control systems containing computers; and handheld devices used to store, transmit, or process unclassified and classified information in the DOE, including the NNSA. The NNSA participates in the DOE CAMS through Under Secretary level infrastructure components that manage CAMS elements in the NNSA sites and offices.

When deployed, the CAMS capability provides asset identification/discovery, threat-based vulnerability assessment and remediation, minimum security configurations, and patch management. The development and governance of CAMS is a living, evolving process, which requires continuous review to measure its effectiveness in meeting stated objectives and to maintain its alignment with the Department's Enterprise Architecture, Information Technology Strategy, Security Strategy, and Capital Planning and Investment Control processes. Emphasis in this concept of operations includes the capability to employ CAMS in all operating environments throughout the DOE.


OCIO identifies needed information and distributes vulnerability, patches and other updates
Transmits to representatives of Undersecretaries and Administrator, NNSA
Transmits to individual program and staff offices the Field and the contractors
Organizations gather information and implement necessary actions
Department-wide continuous monitoring of
– Asset identification/discovery
– Vulnerability assessment / remediation
– Minimum security configurations
– Patch management
Establish Software and Configuration Standards
Identify Threats and Establish Vulnerability Standards
Compare Actual Configuration to Standards
Conduct Vulnerability Assessment
Deploy, Update, and Maintain to Standards
Remediate Vulnerabilities
Report FISMA Metrics
OCIO received needed information and confirmation of actions
Undersecretary/ Administrator representatives aggregate information and confirmation of actions from Program and staff offices and transmits to OCIO
Programs and staff offices transmit information and confirmation of actions to Undersecretary/ Administrator representatives
Organizations report information and implement necessary actions

The CAMS capability fosters a combination of push-pull of both information and activi-

Figure 7. CAMS Capability and Concept of Operations

ties, which, at the Departmental level, supports the systematic and consistent reporting of information and supporting data for FISMA.

CAMS identifies a consistent approach to continuous asset monitoring across all DOE, including NNSA and DOE/NNSA contractor elements. CAMS is based on a federated architecture that supports a blend of DOE, Under Secretary, and site-specific solutions with CAMS infrastructure and DOE-licensed tools for asset identification/discovery, vulnerability assessment and remediation, patch management, and configuration management.

Under Secretaries and sites have the flexibility to select any of the DOE enterprise licensed tools or use existing solutions with the mandatory CAMS infrastructure components. Any Under Secretary specific or site-specific tools used to implement the requirements of CAMS must conform to the data exchange interfaces specified in this document for the tools and elements in the DOE licensed CAMS components.

CAMS includes components and functionality for site-level and system-level vulnerability management, configuration management, asset management, and patch management. The initial implementation of the DOE CAMS allows each DOE site to elect to use CAMS tools throughout the site, or use site implemented solutions that exchange data with the mandatory CAMS infrastructure, or a combination of CAMS and site solutions.

The comprehensive asset management program, depicted in Figure 77, includes technical mechanisms and operational practices, procedures, and processes.

Deliverable:

- Definition and deployment of an asset management tool that can be used to accomplish and report 100 percent inventory of information technology assets in all Departmental elements. (Acquisition of enterprise-licensed CAMS tools in progress).

5.4.3 Automated "OPSEC" Analysis of Web Sites and Servers

Automated review of the information on the DOE and DOE-contractor Web pages is necessary because many users are encouraged by their management to "publish" and share the results of their work. However, very little or no information is available, and no significant analysis has been conducted on the information that is available on the Web pages on who is routinely accessing the information and the potential for obtaining sensitive or classified information by the aggregation of information from multiple Web pages. Sophisticated techniques, such as automated intelligent software agents, operating overtly or covertly, enable a potential adversary to quickly obtain and integrate information from multiple DOE and DOE-contractor Web sites.

DOE and DOE-contractor management need clear policies on establishing Web pages, what information is allowed on the Web pages, who is allowed to access the Web pages, and periodic reviews of Web page content. Automated tools are needed to facilitate the review and analysis of the Web page information. In addition, automated tools and methodologies are needed to detect trends in Web page access to discern patterns of information extraction or collection.

Deliverables:

- Guidance on the creation and management of DOE and DOE-contractor web sites, including content.
- Enterprise licenses for tools to conduct automated analysis of Web site security and content. Tools must be easy to adapt to meet the needs of the program offices and contractor operations.

5.4.4 Awards and Recognition Program

Establish a cyber security awards and recognition program that will reinforce the Department's cyber security goals by publicly recognizing significant contributions by Federal and contractor organizations and personnel.

Deliverables:

- Implementation of a Cyber Security Rewards and Recognition Program.

5.4.5 Certification and Accreditation Assistance

Establish a DOE OCIO-supported C&A advice and assistance function to support implementation of C&A requirements. This function would provide support and assistance to line management and contractor organization in implementing C&A requirements consistent with DOE objectives and expectations.

Deliverables:

- Definition of a process for
- Identifying, and making available, cyber security subject matter experts within the Department to assist line management and contractor organizations with technical or programmatic issue compliance in accordance with Departmental C&A policies, guidance, and bulletins.
- Identifying, and making available, cyber security subject matter experts within the Department to assist line management and contractor organizations in reviewing, correcting existing, and creating new policies and procedures to provide evidence of compliance with Departmental C&A policies, guidance, and bulletins.
- Identifying, and making available, cyber security subject matter experts within the Department to conduct training workshops and

explain DOE policies to line management and contractor organizations to facilitate consistent implementation of C&A requirements.

- Communication of the C&A advice and assistance program across the Department.

5.4.6 Cyber Security Working Group

Establish a senior cyber security management representative in each Under Secretary and Staff Office level organizations. Senior cyber security management representatives at the Under Secretary and Staff Office level would facilitate high-level visibility and management involvement with cyber security.

Deliverables:

- Formal appointment of cyber security leads for the offices of the NNSA Administrator, the Under Secretary for ESE, the Under Secretary for Science, and Staff Offices.
- Define and document the role, and responsibilities for the Cyber Security Working Group.

5.4.7 Communications (internal and external)

Improve communications within DOE and with other government agencies. Communications within and among DOE organizations, and between DOE and other government agencies, should be based on a communications plan for collecting, assimilating, and disseminating classified and unclassified cyber security information to affected parties. Both formal and informal mechanisms are necessary to facilitate communications among the Chief Information Officer, line organizations, intelligence and counterintelligence offices, oversight organizations, and Chief Information Officers of other government agencies.

The communications plan must address the need for near real-time communication of emerging requirements, evolving threats, and cyber security incidents, along with threat and event response feedback mechanisms.

Deliverables:

- Develop and implement a cyber security communications plan.
- Develop and implement standard protocols for communicating with external organizations.

5.4.8 Education, Training, and Awareness

Establish a Department-wide cyber security education and training process. User awareness training materials must be developed, obtained, or adapted for use by Departmental organizations. Training requirements and curricula need to be established to convey

DOE-specific requirements and expectations, along with expectations for job performance of key personnel (e.g., Designated Approving Authority, Information Systems Security Manager, Information Systems Security Officer, and System Administrators). A number of cyber security training courses for IT and cyber security professionals are commercially available and may be applicable to the DOE environment.

Deliverables:

- Training, Education, and Awareness strategy for DOE integrated with national guidance.
- Evaluation of commercially available training courses for applicability to DOE cyber security needs.
- Identify and/or develop effective, job-specific cyber security training curricula and/or courses for DOE and DOE-contractor personnel.
- Establish and maintain a list of recommended cyber security training courses, with links to potential providers.
- Develop and deploy improved computer user awareness training with greater emphasis on cyber security issues.
- Establish a formal process, managed by the DOE OCIO, for documenting and disseminating cyber security lessons learned throughout the DOE complex.

5.4.9 Threat Sharing

Line managers within DOE have been assigned the responsibility to develop cyber security controls to manage risks to an acceptable level. The cornerstone to managing cyber security risks is a full understanding of the threats to the confidentiality, integrity, and availability of information and information systems.

Threat information is available from a variety of public sources (e.g., industry groups) and non-public sources (e.g., CIAC, IG, Homeland Security, intelligence agencies, and counter intelligence functions). All organizations have the ability, and are expected, to maintain awareness of public source information on threats and vulnerabilities. However, managers and staff at many field sites do not have direct access to non-public sources. In particular, cyber security personnel at sites that do not have classified operations need information about cyber security threats that has been classified. The Department's Cyber Security Project Team identified concerns with agency processes to share cyber security threat information. The November 2005 Project Team Report listed specific recommendations for addressing this concern, including "Establishment of a routine process to provide pertinent classified and unclassified threat information to line managers who have risk acceptance responsibility and authority".

An ongoing activity has been initiated to collect and share information via the DOE Counterintelligence organization. Information on cyber threats is collected from across the Department, other government agencies, and the intelligence community. This information is shared weekly with representatives from the Under Secretaries and major Staff Offices in the Department. Early experience with this sharing process has illustrated that the process and mechanisms to transmit, store and communicate the unclassified and classified cyber security threat information across the Department of Energy are not fully developed. As a result of this situation, line organizations are not receiving the threat information needed to effectively manage cyber security risks.

Implementation Issues

- Managers and cyber security staff at some DOE sites do not have secure communication mechanisms (e.g., Entrust certificates) to facilitate secure transmittal of sensitive but unclassified threat information.
- There is no clear understanding of which individuals within DOE Headquarters, field offices and contractors have a need for secure communication mechanisms (e.g., Entrust certificates).
- Managers and cyber security staff at some DOE sites do not have the necessary clearances for access to classified threat information, much of which is at the Secret level.
- There is no clear understanding of which individuals within DOE Headquarters, field offices and contractors have a need for clearances.
- The mechanisms to provide for timely transmittal of classified information do not exist across all DOE organizations. DOE does not have a classified network covering all sites, or uniform access to classified networks managed by external agencies, to facilitate classified information exchange by all sites.
- Many DOE sites do not have the necessary infrastructure for managing classified information (e.g., security organizations and policies, security plans, designated limited areas, safes, and authorized derivative classifiers).
- Mechanisms to allow for classified discussions between DOE organizations do not exist at a significant number of DOE sites (e.g., classified video conference and telephone capabilities).

Deliverables:

- Identification of individuals in DOE headquarters, field offices, and contractor locations that need to receive sensitive or classified threat information;
- Obtain necessary facility authorization and clearances for the identified personnel;
- Documented procedures for threat information sharing;
- Design and implement the protected communications capabilities needed to allow the sharing of sensitive and classified threat information; and

- Threat Statement written for use in accomplishing the DOE Risk Assessment.

5.4.10 DOE Incident Management

The integrated DOE cyber incident management approach, called the Cyber Incident Capability (CIC), provides a strategic view of incident management that focuses on improving the prevention and handling of incidents by integrating incident management into the daily business functions of the DOE organization and establishing strong linkages among those functions. The integrated incident management model combines incident-related services into a single, comprehensive offering that focuses on incident preparedness. The program management component is integral in ensuring each part of the program interacts appropriately with all other parts of the incident management capability and no single part operates independent of the whole program. Ultimately, incident management can evolve into an ongoing, self-improving process implemented throughout DOE to proactively reduce the impact of incidents. The vision for the CIC is

> *A service oriented model for incident detection, response, reporting, and management, with the capability to provide rapid, expert response to incidents and threats across the Department.*

The CIC restructures DOE and NNSA cyber incident detection, response, reporting, and management to enhance the ability to detect, prevent, respond, and recover from computer security events. Another objective is to identify potential risks as far in advance of a potential incident as is possible, and to integrate the identified risks with post-event response and recovery when necessary. Still another objective is to identify the vulnerabilities within the DOE computing enterprise so that they can be mitigated or minimized before they are exploited.

Implementing the CIC provides DOE with the capability to consolidate and correlate security event information from each element of the Department. This capability allows for the effective management of information during the critical moments of initiating incident response and provides a focal point for management of cyber incidents in the Department. It is possible that the CIC could leverage the incident management technologies currently in place to further align their ability to quickly detect and respond to cyber security events.

The CIC will provide

- Trusted and secure communications channels for incident response and management
- A security data warehouse capable of collecting, consolidating, and correlating security events from across the DOE and NNSA
- Centralized incident response management and coordination
- A variety of reporting and information sharing avenues for high level, mid level, and technical employees

- A mechanism to address Federal reporting requirements
- A 24x7 team of security experts focused on the analysis and response to cyber security threats as they evolve
- A rapid-ready force of security incident first responders
- An education and training element capable of regular site visits to assist in the development of a strong incident response procedures

Currently the Department's incident detection and response capabilities consists of separate, inadequately coordinated capabilities, including the Computer Incident Advisory Capability (CIAC), the Cyber Forensics Laboratory (CFL), the NNSA Information Assurance Response Center (IARC), and the Computer Protection Program (CPP) jointly funded by the OCIO and the DOE Office of Counterintelligence.

Deliverable:

- Plan for the funding, development, deployment, and transition to, the CIC within 60 days after acceptance of revitalization plan.

5.4.11 Network Infrastructure Mapping

DOE is deploying the Lumeta network infrastructure mapping capability. The capability analyses network segments from the perspective of systems and applications. It automatically discovers how the network routes and secures application flows and finds the hard-to- isolate systems and connections that may not be in compliance with network management and security mandates. The capability provides unique network intelligence for both security and networking teams. For example, security teams benefit from the capability to determine the overall network security profile for IT infrastructure, validating that network defenses are optimally deployed and in compliance with security strategy. Networking teams benefit from the capability's ability to discover and validate that router and firewall access control lists are corrected implemented, ensuring that only authorized users have visibility to systems and business information. The capability can perform the discovery, analysis and reporting on the operational state of IT infrastructure.

Deliverable:

- Continued deployment of the network infrastructure mapping capability.

5.5 Cyber Security Performance Measurement

5.5.1 Maturity Measurement Methodology

Develop a cyber security methodology for use and implementation across DOE that will define performance measures and metrics to be used to assess an organization's maturity level associated with cyber security and to correlate the effectiveness of accountability to the methodology.

Deliverables:

- Development of methodologies and practices with defined levels of performance.
- Development of processes to assess and measure an organizational status against the methodologies and practices.
- Organizations held accountable for their performance.

5.5.2 Metrics and Reporting

Adequate security of information and the systems that process it is a fundamental management responsibility. DOE management must understand the current status of their cyber security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

Measuring cyber security performance via metrics allows the monitoring of the status of measured activities and facilitates improvement in those activities by applying corrective actions, based on observed measurements. The requirement to measure cyber security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations cite cyber performance measurements in general, and in particular, as a requirement. These laws include the Clinger-Cohen Act and the Federal Information Security Management Act (FISMA). Cyber security metrics will assist in satisfying the annual reporting requirement to state performance measures for past and current fiscal years. Additionally, cyber security metrics can be used as input into the General Accounting Office (GAO) and Inspector General (IG) audits. Existence of a cyber security metrics program will demonstrate DOE's commitment to proactive security. It will also greatly reduce time spent by DOE elements collecting data, which is routinely requested by GAO and IG during audits and for subsequent status updates. The existence of a cyber security metrics program means that the required data will have been tracked, collected, analyzed, and standardized as a part of a regular metrics program operation.

A cyber security metrics program provides a number of organizational and financial benefits. DOE and DOE elements can improve accountability for security by collecting and analyzing cyber security metrics. The process of data collection and reporting will enable management to pinpoint specific technical, operational, or management controls that are ineffective, inefficient, or are not being implemented or implemented correctly. Cyber security metrics can be created to measure every aspect of cyber security program performance. For example, risk assessments, penetration testing, security testing and evaluation, and other security-related activities can be quantified and used to develop metrics. Using the results of the metrics analysis, program managers and system owners can isolate problems, use the collected data to justify investment requests, and then target investments specifically to the areas in need of improvement. By using metrics to target security investments, DOE can get the best value from available resources.

Fiscal constraints and market conditions compel government and industry to operate on reduced budgets. In such an environment, it is difficult to justify broad investments in the IT security infrastructure. Historically, arguments for investing in specific areas of cyber security lack detail and specificity and fail to adequately mitigate specific system risk. Use of cyber security metrics will allow DOE to measure successes and failures of past and current security investments and should provide quantifiable data that will support allocation of resources for future investments. Cyber security metrics can also assist with determining effectiveness of implemented cyber security processes, procedures, and controls by relating results of cyber security activities to the respective requirements and to cyber security investments. Specific examples of such controls include developing policies and implementing procedures, training, infrastructure investments, and network architecture enhancements.

The metrics program implementation plan should be based on the guidance provided by NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems* and tailor that guidance to conform to the requirements of the DOE Cyber Security Program. Under Secretary PCSPs may augment the DOE metrics plan to identify and collect additional information regarding their specific program.

The metric program implementation plan is intended to be a guide for the specific development, selection, and implementation of IT system-level metrics to be used to measure the performance of cyber security controls and techniques as established by the DOE Cyber Security Program. It provides an approach to help management decide where to invest in additional cyber security protection resources or where to discontinue nonproductive controls. It explains the metric process and how it can also be used to adequately justify security control investments. The results of an effective metrics program can provide useful data for directing the allocation of cyber security resources, is expected to simplify the preparation of reports, and aid in meeting the annual requirements of the Office of Management and Budget (OMB) to report the status of the DOE cyber security program.

The metrics program implementation plan should be based on the following basic objectives:

- To develop the information necessary to satisfy statutory reporting requirements (e.g., FISMA),
- To evaluate the effectiveness of the DOE cyber security program,
- To assess adherence to the DOE cyber security program by DOE elements and programs, and
- To provide insight and a quantitative basis for decision making.

Cyber security metrics monitor the accomplishment of the goals and objectives by quantifying the level of implementation of the security controls and the effectiveness and efficiency of the controls, analyzing the adequacy of security activities, and identifying possible improvement actions. Policies and procedures that are ineffective or not cost effective should be identified and eliminated or replaced by cost effective policies and procedures. Specific metrics will be defined to identify ineffective and non-cost effective policies and procedures.

Cyber security metrics can also assist in determining effectiveness of implemented cyber security processes, procedures, and controls by relating results of cyber security activities (e.g., incident data) to the respective requirements and to cyber security investments. Specific examples of such controls include developing policies and implementing procedures, training, infrastructure investments, and network architecture enhancements.

A comprehensive metrics analysis program can provide substantive justification for decisions that directly affect the security posture of an organization, including budget and personnel requests and allocation of available resources, and provide a precise basis for preparing required security reports. Historically, arguments for investing in specific areas of cyber security lack detail and specificity and fail to adequately mitigate specific system risk. Use of cyber security metrics will allow organizations to measure successes and failures of past and current security investments and should provide quantifiable data that will support allocation of resources for future investments.

Metric data is collected annually, semi-annually, quarterly, or monthly. The specific frequency of each metric collection will depend on the life cycle of a measured event. A metric that pertains to the percentage of completed or updated security plans should not be collected more often than semiannually. A metric that pertains to breakable passwords should be collected at least monthly. Continuous measurement will point at continuous implementation of applicable security controls.

Cyber security metrics must yield quantifiable information for comparison purposes, apply formulas for analysis, and track changes using the same points of reference. Percentages or averages are most common, and absolute numbers are sometimes useful, depending on the activity that is being measured.

To be useful for tracking performance and directing resources, metrics need to provide relevant performance trends over time and point to improvement actions that can be applied to problem areas. Management should use metrics to assess performance by reviewing metrics trends, identifying and prioritizing corrective actions, and directing the application of those corrective actions based on risk mitigation factors and available resources. Trends are important indicators early in implementing new policies or procedures.

Deliverables:

- Definition of a DOE Cyber Security Metrics Program Implementation Plan.
- Implementation of DOE Cyber Security Metrics Program Plan at the site, Under Secretary, DOE levels.
- Establishment of a process linking metrics to accountability of Federal and contractor staff and organizations.

5.5.3 Compliance Reviews

The DOE OCIO will conduct periodic compliance reviews of all DOE PCSPs and the implementation those PCSPs. The compliance component of the review will evaluate a PCSP using DOE cyber security policy and guidance issued by the DOE OCIO. To minimize the impact of compliance reviews on the sites, the OCIO will work with the IG and the Office of Independent Oversight and Performance Assessment to reduce, and eliminate where possible, any duplication of efforts. In addition, the OCIO may utilize the results of the IG and the Office of Independent Oversight and Performance Assessment to meet this plan. Results from the compliance review will be provided to the Under Secretary for use in improving the Under Secretary's cyber security program documented in the PCSP. Results from the compliance reviews will be used by the DOE OCIO to improve the DOE cyber security program.

Deliverable:

- Identification of management and technical personnel and funding to support periodic compliance and monitoring reviews of all DOE PCSPs and selected site cyber security programs.
- Compliance And Monitoring Review schedules coordinated with IG reviews and reviews conducted by Office of Independent Oversight and Performance Assessment to minimize impact on site operations.