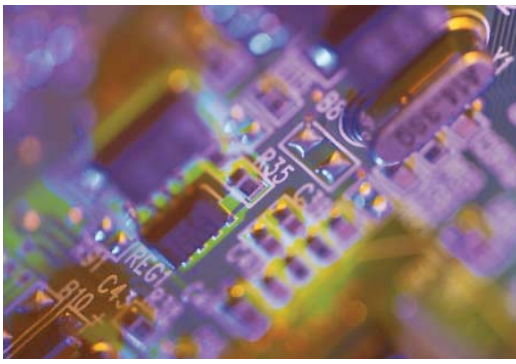
U.S DEPARTMENT OF ENERGY

CYBER SECURITY PROGRAM



CYBER SECURITY STRATEGIC PLAN

FEBRUARY 12, 2007

Table of Contents

INTRODUCTION **4**

CYBER SECURITY STRATEGY OVERVIEW **5**

CYBER SECURITY VISION AND MISSION **7**

CYBER SECURITY STRATEGIC GOALS **8**

GOAL 1: PROTECT DOE INFORMATION AND INFORMATION SYSTEMS TO ENSURE THAT THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF ALL INFORMATION IS COMMENSURATE WITH MISSION NEEDS, INFORMATION VALUE, AND ASSOCIATED THREATS. **8**

STRATEGIC OBJECTIVE 1.1: REDUCE THE RISK OF LOSS, UNAUTHORIZED DISCLOSURE, OR UNAUTHORIZED MODIFICATION OF INFORMATION AND INFORMATION SYSTEMS. 9
STRATEGIC OBJECTIVE 1.2: POLICY AND GUIDANCE IS ADAPTABLE TO MEET CHANGING MISSION NEEDS AND ALIGNED WITH THREATS. 10
STRATEGIC OBJECTIVE 1.3: ALL SYSTEMS AND NETWORKS ARE CAPABLE OF SELF-DEFENSE THROUGH THE DYNAMIC RECOGNITION AND RESPONSE TO THREATS, VULNERABILITIES, AND DEFICIENCIES 12
STRATEGIC OBJECTIVE 1.4: ESTABLISH AND MAINTAIN AN ENTERPRISE CYBER SECURITY ARCHITECTURE
STRATEGIC OBJECTIVE 1.5: IMPLEMENT DOE-WIDE CYBER SECURITY SERVICES. 16

GOAL 2: ENABLE ADVANCED CYBER SECURITY CAPABILITIES **17**

STRATEGIC OBJECTIVE 2.1: LEVERAGE GOVERNMENT, DOE, AND PRIVATE SECTOR RESEARCH AND DEVELOPMENT OF ADVANCED CYBER SECURITY TOOLS AND CAPABILITIES. 17
STRATEGIC OBJECTIVE 2.2: EXPEDITE THE ACQUISITION AND DELIVERY OF INNOVATIVE CYBER SECURITY CAPABILITIES THROUGH INNOVATION. 19

GOAL 3: DEVELOP A CYBER SECURITY KNOWLEDGEABLE WORKFORCE **20**

STRATEGIC OBJECTIVE 3.1: IMPLEMENT A DOE-WIDE CYBER SECURITY TRAINING, EDUCATION, AND AWARENESS PROGRAM 20
STRATEGIC OBJECTIVE 3.2: PROMOTE UNDERSTANDING AND ACCEPTANCE OF CYBER SECURITY CONCEPTS AND PRACTICES THROUGHOUT THE DOE 22

GOAL 4: IMPROVE CYBER SECURITY SITUATIONAL AWARENESS **23**

STRATEGIC OBJECTIVE 4.1: MAINTAIN A DOE-WIDE NEAR-REAL-TIME CYBER SECURITY OPERATIONAL PICTURE 24
STRATEGIC OBJECTIVE 4.2: IMPLEMENT INTEGRATED ENTERPRISE-WIDE ASSET MANAGEMENT CAPABILITY 26

Executive Summary

Over its history, the Department of Energy (DOE) has shifted its emphasis and focus as the needs of the nation have changed. Since the end of the Cold War, the DOE has focused on environmental cleanup of the nuclear weapons complexes, nuclear nonproliferation and nuclear weapons stewardship, delivery of reliable energy supplies, energy efficiency and conservation, alternate energy supplies, and technology transfer. The combination of these changes has led to increased reliance on information technology and interdependencies in a more complex environment requiring near-real time decision-making to successfully respond to challenges.

As the information-based technologies supporting the DOE's scientific, defense, energy, and environmental missions advance, it is becoming increasingly important that security solutions keep pace with the technological advances and their related vulnerabilities, to ward off the threat of loss or compromise of the information assets. The security challenges and threat environment for the DOE's information and information systems are continually evolving as our adversaries increase their skills in seeking access to the DOE's information assets.

To keep pace with this continually changing environment, the DOE must develop comprehensive, risk-based approaches to protect and support our national security, science, and technology missions. Implementing an agile, effective, and cost-efficient approach to cyber security requires the DOE to develop improved and systematic processes, and to leverage technologies to streamline implementation and improve effectiveness of security controls. In this cost-constrained environment, the Department's leadership needs to balance and prioritize security activities, based on risk and mission, and translate its strategies into effective tactical actions.

This Cyber Security Strategic Plan outlines the goals and objectives of the DOE cyber security program to safeguard the DOE's information assets and assure the confidentiality, integrity, and availability of the information vital to achieve the DOE's missions. The details of how the Department will share information, counter new and evolving threats, and develop new methods for protecting information and information systems will be defined in the policies and in the mission-centric Senior DOE Management Program Cyber Security Plans (PCSPs).

This strategic plan contains the goals and strategic objectives for the DOE Cyber Security program. Each strategic objective is organized into near-term, mid-term, and long-term element. The elements are "time boxed" with near-term elements expected to be addressed in the next 12 months, mid-term elements addressed in the next 18-24 months, and the long-term elements addressed in the next three years.

INTRODUCTION

Since its beginning in the World War II Manhattan Project, the Department of Energy (DOE) has had a responsibility of providing the Nation with the necessary science and technology to develop and maintain what we have come to know as "our way of life" and to protect our national and economic security. Through highly advanced information systems and leading edge research, DOE has become a world-class leader. DOE laboratories house sophisticated facilities where engineers and scientists perform research spanning DOE's energy, science, national security, and environmental quality missions.

The research and development of advanced technologies supporting its missions have made the DOE and its laboratories an increasingly attractive target to those who seek its technologies and our national security information. These security challenges and threats for the DOE's information and information systems are increasing in number, complexity, and sophistication. In this changing environment, the DOE must develop and continuously refine agile strategic approaches to advancing, integrating, and automating its protection and response capabilities.

This Cyber Security Strategic Plan establishes a roadmap for improving cyber security in the DOE over the next three years. This Plan describes how the DOE will protect and share information, counter new and evolving threats, transform its workforce, and support the development of mission-oriented specific guidance to effectively and seamlessly integrate security into everyday operations. This Strategic Plan addresses cyber security practices and approaches, with near-term objectives being addressed in the next 12 months, mid-term objectives addressed in the next 18-24 months, and long-term objectives addressed over the next three years.

This Strategic Plan is a living document; the vision, goals and objectives of this plan will be reviewed at least annually for relevancy, currency, and applicability and modified, as necessary, to keep pace with the changing environment and address significant challenges.

DOE's ability to successfully achieve the objectives in this plan requires the continued commitment and mandate from Senior Leadership and the cooperative support of all members of the DOE community.

CYBER SECURITY STRATEGY OVERVIEW

Department of Energy Mission

The DOE's overarching mission is "Discovering the solutions to power and secure America's future." The DOE has five strategic themes towards achieving its mission:

- Energy Security: Promoting America's energy security through reliable, clean, and affordable energy
- Nuclear Security: Ensuring America's nuclear security
- Scientific Discovery and Innovation: Strengthening U.S. scientific discovery, economic competitiveness, and improving quality of life through innovations in science and technology
- Environmental Responsibility: Protecting the environment by providing a responsible resolution to the environmental legacy of nuclear weapons production
- Management Excellence: Enabling the mission through sound management

Department of Energy Information Technology Vision

DOE's information technology (IT) vision aims to affect governance and processes in order to provide access to modern, reliable, and secure IT infrastructure and systems that support and enhance DOE's mission in the 21st century. Figure 1 below identifies the Goals and Objectives of the Information Resources Management (IRM) Strategic Plan. As part of the IT vision, DOE continues to implement and maintain a comprehensive and effective cyber security program to protect the DOE's classified and unclassified information and IT assets.

Figure 1 — Information Resources Management Strategic Goals

Strategic Goal 1: Enhance the value of DOE information and products for mission effectiveness
Objective 1: Enable mission programs and operations with effective technology products and information.
Objective 2: Partner and Support the Presidential e-Government Initiatives.
Objective 3: Support the Department's e-Government Activities.
Strategic Goal 2: Institute a robust IT governance program within DOE
Objective 1: Enhance the Capital Planning and Investment Control (CPIC) Processes for IT to maximize portfolio value and performance.
Objective 2: Develop and Maintain an Enterprise Architecture (EA) that is reliable, adaptable, scalable, and driven by business and technology requirements.
Objective 3: Ensure effective IT project performance.
Objective 4: Implement an Enterprise Licensing Agreement Program.
Objective 5: Recruit, develop, and retain a qualified, professional IT workforce.

Strategic Goal 3: Improve cyber security by reducing the number of vulnerabilities at DOE
Objective 1: Improve compliance with Federal Information Security Management Act of 2002 (FISMA) and all other cyber-security Government-wide regulations, policies and procedures.
Objective 2: Implement a comprehensive DOE-wide security-management program to improve cyber security.
Objective 3: Implement a comprehensive vulnerability management program to identify and mitigate vulnerabilities in DOE information systems.

In FY06, the DOE developed a new Strategic Plan that will meet the Nation's Energy and National Security challenges into the future. The DOE Strategic Plan provides direction for the next 25 years by "discovering the solutions to power and to secure America's future." The DOE has further integrated its long-term and intermediate goals into the annual performance budget. This performance structure establishes the necessary links between the DOE Strategic Plan's goals and the DOE's annual budget, performance metrics, and performance reporting. Table 1 below illustrates the strategic goal for each of the five business lines to which the performance structure ultimately aligns.

Table 1 — Alignment of DOE Business Lines and Strategic Goals

DOE Business Lines	DOE Strategic Goal
Energy Security	Promoting America's energy security through reliable, clean, and affordable energy
Nuclear Security	Ensuring America's nuclear security
Scientific Discovery and Innovation	Strengthening U.S. scientific discovery, economic competitiveness, and improving quality of life through innovations in science and technology
Environmental Responsibility	Protecting the environment by providing a responsible resolution to the environmental legacy of nuclear weapons production
Management Excellence	Enabling the mission through sound management

CYBER SECURITY VISION AND MISSION

This Cyber Security Strategic Plan establishes this vision and mission for the DOE Cyber Security Program with goals, objectives, elements, and outcomes to ensure the DOE's information and information systems are protected.

The DOE Cyber Security vision is:

> ***An agile, effective, and cost-efficient approach to cyber security aligned with current threats and adaptable to the DOE's missions***

While supporting the cyber security mission to:

> ***Enable improved DOE mission accomplishment while strengthening the protection of systems and data***

Successful accomplishment of the goals and objectives will result in realizing the vision and the transformation of our operations, technologies, processes, and people across the DOE. We aim to achieve the following.

Operations

- Program managers, users and supporting personnel will have confidence in the information needed to achieve their missions.
- Decision makers will share a seamless, enterprise-wide, and common view of information, networks, and systems, allowing them to jointly make decisions.
- DOE's secure enterprise architecture will allow appropriate sharing of information and knowledge throughout the DOE and enable multiple levels of information sharing across security environments.

Technologies

- Cyber security capabilities will be dynamic, sufficiently robust, and agile - reconfigurable on demand, available, and consistently controlled at all points of access, with reduced possibility for human and machine error.
- Cutting-edge protection, detection, and response technologies will be rapidly deployed across all DOE systems and networks, outpacing adversaries' efforts to exploit vulnerabilities.

Processes

- DOE processes and governance principles will support mission accomplishment in a networked environment, will be continually improved, and will be sufficiently dynamic and agile to accommodate rapidly changing needs.

- DOE's cooperative relationships with academia, industry, and research and development (R&D) organizations will allow rapid integration of available technologies and embed enhanced hardware and software assurance solutions in future capabilities.

People

- Cyber security personnel will consistently demonstrate the highest skill levels in managing and deploying the latest technologies and methods.
- The entire DOE workforce will recognize the importance of cyber security, understand their role in it, and will be constantly vigilant.

CYBER SECURITY STRATEGIC GOALS

Goal 1: Protect DOE information and information systems to ensure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats.

Data protection must begin with the creation of information, with particular focus on defining and documenting protection levels and access control decisions. Protection must be assured throughout the life cycle of the data: creation, modification, storage, transport, and destruction. Being part of the myriad of interconnected DOE networks and the DOE enterprise means that information (e.g., data, metadata) routinely flows in and out of a network through numerous access points. This separation of information from systems requires that the information must receive adequate protection, regardless of its physical or logical location, or its method of transportation.

A critical factor in ensuring adequate protection for all data is the responsive updating and application of policy and guidance to address the latest changes in technologies while defending against the latest new and developing threats. Equally important is the necessity to ensure that the policies and guidance provide sufficient flexibility to allow their adaptation to the diverse missions across the DOE. In addition, ensuring the protection of data everywhere within the enterprise requires partnerships and combined efforts with other components of the security community (i.e., Intelligence, Counterintelligence, Operations, Physical/Personnel security, and critical infrastructure protection) to provide an integrated systems security posture.

Cyber security policies define the requirements and procedures required for the effective achievement of the DOE's cyber security mission. Enhanced through guidance and performance metrics, DOE policy drives the program's implementation through Senior DOE Management[1]. The structure is focused on high-level policy supported by supplemental technical and management guidance at the Departmental Level. Through their

[1] Senior DOE Management includes the DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and the DOE Chief Information Officer

cyber security programs documented in their Program Cyber Security Plans (PCSPs), Senior DOE Management implements the program defined in the policy and guidance for their organizations. The DOE policy and guidance structure includes:

- DOE Directives System – Process for developing and issuing formal Orders, Manuals, and Notices.
- Technical and Management Requirements – DOE CIO direction for implementation in Senior DOE Management cyber security programs.
- Bulletins – DOE CIO guidance addressing responses to immediate issues.

Ensuring the protection of data anywhere across the enterprise requires partnerships and combined efforts with other components of the security community (i.e., Intelligence, Counterintelligence, Operations, Physical/Personnel security, and critical infrastructure protection) in order to provide an integrated systems security posture.

Strategic Objective 1.1: Reduce the risk of loss, unauthorized disclosure, or unauthorized modification of information and information systems.

Near-Term—Revise policy and investigate measures to improve the DOE corporate cyber security regime. Work with other Government Agencies and private industry to enhance the DOE corporate cyber security regime through cooperative interaction and cyber security program enhancements.

Elements

- Ensure that DOE cyber security policies and guidance provide for common protection of information across the DOE.
- Promote changes and enhancements to DOE and US Government cyber security policies to enable the implementation of next-generation information and systems and processes.
- Implement training to enhance DOE Federal and Contractor employees' understanding of, and participation in, the DOE Cyber Security Program.
- Ensure DOE-wide information and cyber security architectures integrate transparent security processes into next-generation systems.
- Involve senior management and cyber security staff in the development of DOE policy and guidance that provides the flexibility to meet the security and mission needs of DOE.
- Increase interaction and cooperation among CIO, security, counterintelligence, intelligence and program organizations in the identification and mitigation of cyber threats.
- Define performance measures to monitor and evaluate the implementation of cyber security by all DOE organizations.

Mid-Term—Refine and institutionalize DOE cyber security policy, guidance, and practices consistent with program requirements, evolving threats, and evolving DOE strategies. Facilitate improvements in DOE and US Government-level cyber security policies through the sharing of innovative risk management knowledge and tools.

Elements

- Disseminate new and improved cyber security policies, guidance, practices, and tools to all DOE elements.
- Design new cyber security policies to meet implementation constraints, including technical, programmatic, regulatory, and resource-driven requirements.
- Involve senior management and cyber security staff in the development of DOE policy and guidance that provides the flexibility to meet the security needs of DOE.
- Challenge the cyber security policy staff to develop professionally into the next generation of experts and leaders.
- Use performance measures to monitor and evaluate the implementation of cyber security by all DOE elements.

Long-Term— Advance a cyber security program that is integrated into DOE's scientific, engineering, production, and business processes, and that ensures information is routinely and reliably available for use by all authorized DOE entities. The program allows for the authorized sharing of information assets while providing appropriate protection and managing risk in a manner transparent to the end user.

Elements

- Increased use of common implementation of DOE policies and guidance across all DOE operating units.
- Increased interaction and information sharing concerning policy, guidelines, and practices with other agencies that aid in DOE information protection that is consistent with other Government agencies.

Success Measures

- Reduction in the number of cyber security incidents.
- Common implementation of DOE and US Government policies and guidance across all DOE operating units in support of national security, environmental, science, and internal business programs.
- Increased collaborative activity across the DOE operating units in the identification and mitigation of active threats and perpetrators.
- DOE information protection strategies are consistent with other Government agencies.

Strategic Objective 1.2: Policy and guidance is adaptable to meet changing mission needs and aligned with threats.

Near-Term – Provide Senior DOE Management with a framework of technical and management requirements that are compliant with US Government requirements and good best practices for applying cyber security controls to meet mission-specific objectives.

Elements

- Solicit support from Senior DOE Management to shape policy and guidance that is compatible with mission accomplishment.
- DOE federal and contractor community are engaged in policy and guidance development by solicitation of recommendations, comments, and "best practices" during policy and guidance development and revision.
- Construct DOE-level policy and guidance that are risk-based and consistent with, and responsive to US Government-level security policy, guidance, and related initiatives.
- Policy and guidance are responsive to US Government-level, DOE-level, and DOE- program specific threats, and implementation of next-generation information and knowledge management systems and processes.
- Structure cyber security governance and accountability to satisfy the flexibility and agility demands of the enterprise and to enable the effective and cost-efficient implementation by Senior DOE Management in their program environments.
- DOE cyber security policies, guidance, and processes support consistent protection of information and information systems, thereby reducing the risk of unauthorized disclosure, loss, or modification of classified and unclassified information.
- Define performance measures for policy and guidance effectiveness.

Mid-Term–Define and deploy a repeatable, responsive, and managed process for refining policy and guidance based on US Government requirements and guidance, internal and external best practices, and lessons learned.

Elements

- Refine, streamline, and enhance policy with internal and external lessons learned and good practices.
- Use feedback from compliance reviews, metrics, internal program oversight, and external program oversight to improve policy and guidance.
- Ensure that cyber security governance and accountability continue to satisfy the flexibility and agility demands of the enterprise and enables the effective and cost-efficient implementation by Senior DOE Management in their program environments.
- Ensure that DOE policy and guidance remains consistent with National requirements and guidance.
- Measure policy and guidance effectiveness through a performance measurement program.
- Expand involvement of the DOE federal and contractor community in policy and guidance development.
- Ensure that policy and guidance are responsive to US Government-level, DOE-level, and DOE program-specific threats.

Long-Term—Provide clear and consistent risk-based cyber security policy and guidance that incorporates good practices, meets US Government requirements and guidance, and is responsive to evolving cyber security threats

Elements

- Use feedback from compliance reviews, metrics, internal program oversight, and external program oversight to improve policy and guidance.
- Ensure that policy and guidance remain consistent with National requirements and guidance, threat assessments, and implementation limitations.
- Institutionalize communication with other Government Agencies regarding cyber security policy and practices.
- Continue and refine measurement of policy and guidance effectiveness through the performance measurement program.

Success Measures

- Cyber security governance processes and accountability satisfy the flexibility and agility demands of the enterprise and enables effective and cost- efficient implementation by Senior DOE Management.
- A mature, agile DOE cyber security policy and guidance development process integrates collaboration between the DOE Office of the Chief Information Officer (OCIO) and Senior DOE Management.
- Cyber security policy and guidance is interpreted and implemented consistently across the DOE enterprise.
- Reduction in number of cyber security incidents.
- Reduction in repeat findings across DOE.

Strategic Objective 1.3: All systems and networks are capable of self-defense through the dynamic recognition and response to threats, vulnerabilities, and deficiencies

DOE systems and networks are constantly under attack and must be continuously defended. To ensure success, defensive mechanisms must be an integral part of the design and deployment of systems and networks across the enterprise. In addition, capabilities must be deployed to react and respond to attacks. The application of protection measures defined in DOE cyber security policy and guidance, integrated with sound system security engineering practices across the enterprise, will reduce potential points of failure and provides consistent security measures across the enterprise.

To accomplish the goal of self-defense, DOE networks will require a significant increase in the autonomous abilities of every "node" and "link" in the system to:

- Identify and correct suspicious or unwanted behavior.
- Self-heal when penetrated or damaged.
- Detect and respond to the differences between legitimate and suspicious demands for system and network resources.

Near-Term – Defend DOE information systems and networks by recognizing and reacting to threats and vulnerabilities.

Elements

- Construct and promulgate Computer Network Defense[2] (CND) policies across the enterprise that achieve an optimal readiness posture, as technology progresses, against threats posed by the outsider "nation state" attacker as well as insider.
- Identify and deploy CND tools and capabilities in a coordinated manner at enclave, local area network and facility levels.
- Define DOE incident management policies and guidance to effectively utilize developed CND tools and capabilities to react and respond to events.
- Identify and deploy forensic tools and capabilities in a coordinated manner at enclave, local area network and facility levels.
- Mitigate the insider threat across DOE through the implementation of advanced tools, processes, and operational capabilities.
- Deploy a continuous asset management capability within the DOE complex.
- Continuously assess and evaluate DOE information systems and networks.
- Design and deploy a DOE-wide Indications and Warning (I&W) capability to warn of potential or ongoing attacks against the enterprise.
- Share attack information with security, counterintelligence, intelligence and Senior DOE Management.

Mid-Term –Integrate leading edge security solutions that blend security incident management systems and Intrusion Detection Systems (IDS) with Intrusion Prevention Systems (IPS) to ensure the information on DOE information systems and networks is defended.

Elements

- Build relationships with key vendors, other agencies, and DOE programs to develop and deploy advanced sensor technologies to provide early warning threat notification.
- Implement an integrated enterprise-wide incident detection, prevention, analysis, response, and recovery capability.
- Deploy network security solutions that actively degrade malicious activity propagation.
- Deploy post mortem forensic systems capable of gathering and storing historical and real-time data and integrating the information to allow for chronological analysis of events and impacted systems.
- Identify security solutions that can be tailored based on Senior DOE Management business requirements.

Long-Term – Deployment of CND protection, detection, and reaction mechanisms for DOE systems and networks and adaptive configuration management. (Adaptive configuration management is a critical capability that includes both active and passive defenses necessary to "correctly" respond appropriately to legitimate but changing demands while simultaneously defending against adversary-induced threats.)

[2] Computer Network Defense is the collective term for the policies, tools, practices and capabilities applied to defend the DOE computer networks and information systems against external and insider attacks.

Elements

- Deploy information systems or applications capable of degrading malicious activity and analyzing and controlling information flows within networks and across the enterprise.
- Deploy information systems or applications capable of assuming control of ongoing malicious activity communication sessions, simulating the network environment and replacing internal services on the fly without noticeable impact on perpetrator behavior or network performance.
- Deploy analysis and response management systems capable of gathering, integrating, analyzing data and controlling the information systems and applications used to control malicious activity.
- Deploy real-time and post mortem forensic systems capable of gathering and storing historical and real-time data and integrating the information to allow for chronological analysis of events and impacted systems.

Success Measures

- DOE Headquarters, Senior DOE Management organizations, and their operating units are equipped with advanced systems to monitor, detect, analyze, and respond to threats.
- DOE Headquarters, Senior DOE Management and their operating units have near real-time management and monitoring capabilities of IT assets.
- Reduction in network intrusions across the enterprise.
- IT security technologies are acquired and deployed that blend intrusion detection, prevention, and active defense capabilities.
- Integrated enterprise incident management.
- Integrated enterprise active defense capability.

Strategic Objective 1.4: Establish and maintain an enterprise cyber security architecture

Given its federated structure, the DOE 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. To ensure that information is protected as it flows through the enterprise, an end-to-end cyber security architecture must be developed and DOE must develop new protection solutions to support the wide spectrum of user needs. The keystone to a secure computing environment is a well-maintained and documented technology management plan that clearly defines the purpose, scope, and usage of the cyber security architecture. This baseline leads to the successful implementation of security controls throughout an operating environment, or computing enclave.

Installing well-defined, high-level DOE structure, processes, and principles enables DOE to successfully manage and secure the technology it employs. These processes and principles include:

- Architectural Guidance – Definition of the DOE cyber security architecture that provides the structure for review and acceptance of new technologies.
- Enterprise Licensing – Obtaining cyber security solutions that incorporate the needs of Senior DOE Management and their operating units.
- Technology Review – Process for standardized approach to the identification of new technologies that may be of interest to Senior DOE Management and their operating units.

- Technology Development – Process for initiating the development/introduction of a new systems or technology that may be beneficial to Senior DOE Management and their operating units.

Near-Term - Develop and begin implementation of a DOE cyber security architecture that captures the strategic vision of the cyber security program.

Elements

- Develop and document a cyber security architecture that provides the framework for integrating separate products and tools to meet current threat needs and anticipate future threats, technology direction, and mission needs and integrate security processes transparently into next-generation information and knowledge management systems.
- Develop a comprehensive DOE "to-be" cyber security architecture roadmap.
- Develop and publish DOE OCIO guidance on transition to the "to-be" architecture.

Mid-Term – Evolve the definition and implementation of the cyber security architecture accompanied by an explicit business process that ensures the integration of cyber security into all information systems from their inception.

Elements

- Develop and publish DOE OCIO guidance on development procedures, product selection, implementation, and management for transitioning to the "to-be" security architecture.
- Enhance the cyber security architecture to meet the specific needs of each Senior DOE Management organization, with a focus on the relationships among people, processes, information, and technologies.
- Develop a phased transition plan that provides a roadmap for modernization and standardization that can be traced directly to the "to-be" architecture, missions and business goals, and is integrated with Capital Planning and Investment Control processes, with measurable plans, schedules, and budgets.

Long-Term –Institutionalize a DOE cyber security architecture that provides the framework to enable secure communication, protect agency business processes and information resources, and ensures that new methods for delivering services are secure when deployed. The results of evolving this architecture include increased interoperability, compatible security solutions, and ensured assurance of information confidentiality, integrity, and availability throughout the enterprise.

Elements

- Focus the cyber security architecture to meet the needs of the DOE operating unity and the inter-communication needs of the DOE, with a focus on the relationships among people, Government organizations, processes, information, and technologies.

Success Measures

- IT business decisions are aligned with the DOE cyber security architecture.

Strategic Objective 1.5: Implement DOE-wide cyber security services.

The DOE cyber security program provides various services, Figure 1, through several key elements that focus on outreach, information sharing, and advice and assistance. The aim of these elements is to develop an intelligent, proactive approach to mitigating the security threat to the DOE.

If advice and assistance is required by any part of the DOE, the OCIO is available to assist in a variety of activities, such as risk mitigation, threat identification, or incident recovery.

Near-Term—Develop or improve processes to meet common cyber security needs or provide specialized support.

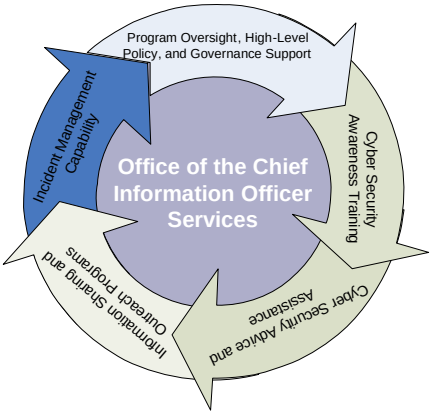


Figure 1. CIO Services

Elements

- Cyber Security Communications – Process for the dissemination of cyber security threat and lessons learned information across the DOE.
- Certification and Accreditation Assistance – The DOE OCIO provides assistance as requested for certification and accreditation activities.
- Cyber Security Advice and Assistance – The DOE OCIO provides requested support for various cyber security activities.

Mid-Term—Maintain, and identify new, common cyber security needs and support services.

Elements

- Maintain communications, certification and accreditation assistance, and advice and assistance services.
- Expand Cyber Security Advice and Assistance to include providing implementation options to meet mission needs.
- Identify opportunities for additional cyber security services.

Long-Term— Maintain, and identify new, common cyber security needs and support services. Identify, and acquire new ideas and concepts for DOE-wide cyber security services. Facilitate collaborative interactions to identify common cyber security services needed across the DOE.

Elements

- Maintain communications, certification and accreditation assistance, and advice and assistance services.
- Identify opportunities for additional cyber security services.

Success Measures

- Senior DOE Management and operating units request support services
- Senior DOE Management and operating units recommend additional support services

Goal 2: Enable advanced cyber security capabilities

The ever-changing and evolving information technology industry stresses DOE's processes and challenges them to keep pace. Maintaining an edge over our adversaries demands that we transform the mechanisms we use to develop and deliver new and dynamic cyber security capabilities becomes more responsive to ever-changing needs. Agility in our cyber security policies, guidance, and practices must be a goal for every process for DOE to maintain this competitive edge. Continuous improvement is mandated. The continuous improvement approach places great importance on harvesting and prioritizing ideas and the rapid development and deployment of concepts and capabilities to enable constant preparation, shaping, and execution of our responses to the environment.

Transforming cyber security capabilities depends heavily on the ability to influence processes the DOE uses to create, assess, test, and implement new ideas. Developing new approaches to problem solving depends on the synergy between each process as an idea progresses from concept to reality. The focus of this goal is to foster innovation and influence the planning and acquisition processes to further the cyber security mission and support the DOE missions as they may change.

Strategic Objective 2.1: Leverage Government, DOE, and private sector research and development of advanced cyber security tools and capabilities.

Near-Term—Develop relationships with private industry and other Government agencies to identify advanced cyber security tools and capabilities for possible use within the DOE.

Elements

- Develop and implement a cyber security R&D program focused on specific DOE cyber security needs.
- Develop partnerships and relationships with intelligence community organizations conducting cyber security tool and capability research and development.
- Identify current threats, document currently implemented countermeasures, and provide the foundation for future research and development efforts in threat management.
- Share the results of cyber security tool and capability research and development by DOE organizations.
- Develop partnerships and relationships with private industry organizations conducting cyber security tool and capability research and development.
- Enhance information sharing between intelligence groups and safeguards and security designers to ensure that emerging threats are being addressed and mitigated.

- Promulgate policies and guidance that reflect the range of current and projected threats to ensure the identified threat spectrum is addressed and the requisite research and development efforts provide the appropriate technologies in the relevant disciplines.

Mid-Term—Support the prototype use and deployment of advanced cyber security tools and capabilities developed by organizations within the DOE, by other Government organizations, and private industry. Sponsor advanced cyber security tool and capability technology development in DOE.

Elements

- Establish agreements with the intelligence community and private industry organizations conducting cyber security tool and capability research and development for DOE to test, prototype, and possibly deploy these cutting-edge cyber security tools and capabilities across the DOE.
- Integrate advanced security technologies and capabilities that are adaptable to changes in threat conditions into the cyber security architecture.
- Institutionalize information sharing between intelligence groups and safeguards and security designers to ensure that emerging threats are being addressed and mitigated.
- Develop a DOE cyber security technology development program plan.
- Identify projected threats, document proposed countermeasures, and provide the foundation for research and development efforts in threat management.

Long-Term— Establish frequent interactions among DOE organizations, other Government agencies, and private industry organizations to exchange information on the design, development, prototype use, and deployment of advanced cyber security tools and capabilities. Sponsor advanced cyber security tool and capability technology development in DOE.

Elements

- Integrate into information systems advanced security technologies and capabilities that are adaptable to changes in threat conditions.
- Enhance and formalize effective relationships and agreements with the intelligence community and private organizations conducting cyber security tool and capability research and development for DOE to test, prototype, and possibly deploy cyber security tools and capabilities across the DOE.
- Develop a rolling ten-year threat outlook to ensure that postulated threats are being considered in the IT research and development cycle.
- Integrate advanced security technologies and capabilities that are adaptable to changes in threat conditions into information systems.
- Institutionalize information sharing between intelligence groups and safeguards and security designers to ensure that emerging threats are being addressed and mitigated.
- Publish a DOE cyber security technology development program plan focused on unique DOE cyber security needs.

Success Measures

- Identification, successful prototyping, and deployment of advanced cyber security tools and capabilities developed by DOE and other organizations.
- Successful application of protection technologies and procedures that are transparent to system and facility users and enhance protection reliability over current systems.
- Identification and isolation, removal or replacement of DOE information systems that cannot or do not incorporate capabilities that meet minimum protection requirements.
- Introduction of adaptable cyber security technologies to address emerging and postulated threats.
- Cooperation and information sharing between the intelligence and cyber security communities to ensure that emerging and postulated threats are being identified.

Strategic Objective 2.2: Expedite the acquisition and delivery of innovative cyber security capabilities through innovation.

Near-Term—Develop or improve processes to identify common cyber security needs where enterprise investments are cost-effective.

Elements

- Facilitate identification of ideas for new and dynamic cyber security capabilities suitable for enterprise investment.
- Identify, review, test and evaluate technologies against cyber security needs for experimentation, implementation, or investment.
- Improve programs and processes fundamental to risk-based implementation of COTS/GOTS solutions.

Mid-Term—Routinely identify common cyber security tools and capabilities through collaborative interaction across the DOE and through the application of the cyber security architecture.

Elements

- Facilitate identification and communication of ideas for new and dynamic cyber security capabilities suitable for enterprise investment.
- Identify, review, test and evaluate technologies against cyber security needs for experimentation, implementation, or investment.
- Sponsor DOE-wide development of requirements, procurement strategies, acquisition, and deployment of common DOE-wide cyber security tools and capabilities.

Long-Term— Improve our processes to develop, identify, and acquire new cyber security concepts, conduct cyber security research and development, and deploy cutting-edge cyber security capabilities. Facilitate collaborative interactions to identify common cyber security tools and capabilities across the DOE and ensure that the resulting policies, guidance, and/or recommended tools are integrated into Senior DOE Management and DOE cyber security programs.

Elements

- Institutionalize the identification and communication of ideas for new and dynamic cyber security capabilities suitable for enterprise investment.
- Collaborate with Senior DOE Management cyber security programs to identify, review, test, and evaluate technologies against cyber security needs.
- Sponsor the implementation and maintenance of DOE-wide development of requirements, procurement strategies, acquisition, and deployment of common DOE-wide cyber security tools and capabilities.

Success Measures

- Ideas for new and dynamic cyber security capabilities suitable for enterprise investment are identified and shared with all Senior DOE Management cyber security programs.
- Collaboration among Senior DOE Management and DOE cyber security staff to identify, review, test and evaluate technologies against cyber security needs.
- The DOE cyber security program sponsors DOE-wide development of requirements, procurement strategies, acquisition, and deployment of common cyber security tools and capabilities.

Goal 3: Develop a cyber security knowledgeable workforce

As we prepare for the future, we are continually reminded that people are the foundation of the DOE and also are the greatest resource in protecting its information and information systems. Establishing a comprehensive training, education, and awareness program helps ensure that personnel in all levels of the Department understand their roles and responsibilities in protecting the DOE's information assets and are prepared to react to today's and tomorrow's threats. In todays increasingly more capable and hostile threat environment, every employee plays an important role. The difference between being a vulnerability and being an element of defense-in-depth security can be measured in the quality of training, education, and awareness of employees.

Training, education, and awareness programs also support the development of a professional workforce with the knowledge, skills, and abilities to prevent, deter, and respond to threats against DOE information and information systems. Cyber security training, education, and awareness programs provide critical management and operational support to the DOE's overall Cyber Security Program.

Strategic Objective 3.1: Implement a DOE-wide cyber security training, education, and awareness program

Near-Term – Increase cyber security awareness across the DOE and implement a cyber security-focused, professional development and proficiency program that will provide the DOE with needed managerial and technical skills needed to support and protect current and projected mission requirements. The program will address the technical and role-specific training to support Information System Security Officers (ISSO), Cyber security managers, Certification Agents, Designated Approving Authorities (DAA) and their staff.

Elements

- Measure cyber security awareness of personnel (via gap analysis or other method) to determine areas of needed improvement.
- Establish cyber security training, education, and awareness at all levels throughout the DOE.
- Integrate cyber security as part of program, project, and management briefings and communications.
- Infuse cyber security awareness and concepts into other disciplines.
- Provide technical and job-specific training based on the guidelines of National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*.
- Institute a Professional Development Program (PDP) that supports DOE's specific technical and mission needs through core and career-specific curricula.
- Develop technical competencies for inclusion into the DOE Technical Qualification Program functional area standards.
- Develop employee recognition, recruiting, and retention programs.
- Develop and promote educational opportunities with institutions of higher education and other Government agencies.
- Recruit interns and other entry-level employees to expand the experience horizon.
- Cross- train cyber security personnel at other programs and facilities.

Mid-Term - Continue to develop and update the PDP to meet changing requirements, work environments and security concerns. Interlace the PDP with a Succession Plan to ensure that employees not only receive necessary training and education, but also that they are sufficiently experienced and prepared to advance into positions being vacated.

Elements

- Promote expanded cyber security training, education, and awareness throughout the DOE.
- Establish baseline certification across the enterprise by leveraging professional certification programs, such as Certified Information System Security Professional (CISSP) and Global Information Assurance Certification (GIAC).
- Establish a career path tracking capability to ensure advancement opportunities are available to cyber security staff.
- Continuously review feedback against strategic workforce planning goals and update the PDP as policy and technology changes warrant.
- Identify human capital needs through workforce planning and analysis in order to understand current workforce skills, retirement impacts, and present and organizational workforce needs.
- Further enhance and institutionalize advanced cyber security training and education into the career path for practitioners and managers and provide incentives for achieving their qualifications.
- Expand partnerships with other Government agencies and institutions to provide job-specific training, management and crosscutting training opportunities.
- Leverage the Senior DOE Management cyber security community to educate users.

- Tailored training for specific program issues (for example, scientists visiting for a short time at a laboratory).
- Establish and maintain a program to retain experienced cyber security personnel within the DOE.
- Develop and acquire facilities to train and support PDP participants.

Long-Term – Provide cyber security training, education, and awareness for all DOE contractors and employees, from entry level to and Senior DOE Management. Technical training and education focuses on system and network administrators and personnel performing maintenance functions on DOE workstations, systems and networks, and professional development for ISSO, Cyber security managers, Certification Agents, DAAs and their staff.

Elements

- Incorporate career fields, beyond the traditional safeguards and security programs, into the intern program (e.g., Systems Engineers, Counterintelligence, and Emergency Management) to provide a full range of career and professional development services.
- Expand partnerships with other Government agencies and institutions to provide job-specific training, management, and crosscutting training opportunities.
- Maintain a pipeline of diverse, qualified candidates to mitigate security organizations' human capital needs.

Success Measures

- A PDP to educate and retain experienced cyber security personnel within the DOE.
- Institutionalized processes for continuing education, career advancement, and certification.
- A DOE-wide cyber security training, education and awareness program that supports current and projected mission requirements and succession plans.
- A federal and contractor federal workforce that is well -versed in cyber security-related topics and flexible enough to respond to additional responsibilities and changing conditions.
- Balanced workforce of cyber security practitioners with the right number of personnel with the right skill sets to support effective security.

Strategic Objective 3.2: Promote understanding and acceptance of cyber security concepts and practices throughout the DOE

Near-Term – Increase cyber security awareness among all employees.

Elements

- Include cyber security elements into the DOE Technical Qualification Program functional area standards.
- Senior DOE Management provides Cyber Security Training, Education, and Awareness programs throughout the DOE complex.
- Establish methods, processes, and tools for measuring the effectiveness of awareness activities.

Mid Term – Incorporate cyber security responsibility awareness and acceptance into the core work values of all employees.

Elements

- Develop collegial, interpersonal delivery methodologies for cyber security awareness information.
- Encourage personal acceptance of cyber security responsibilities by all Federal and contractor staff.

Long-Term – Incorporate cyber security responsibility awareness and acceptance into the core work values of all employees by continuously improving the awareness program as required by the changing threat environment and advances in security technology.

Elements

- Continuously review and modify Cyber Security Training, Education, and Awareness program to address the changing threat environment and technological advances in information security.
- Deploy multi-media delivery methodologies for cyber security awareness information.
- Encourage personal acceptance of cyber security responsibilities by all Federal and contractor staff.

Success Measures

- Demonstrated willingness to take action in response to cyber security perpetrator activity as reflected in increased reporting of concerns by employees.
- Demonstrated willingness of cyber security personnel (Federal and contractor staff and systems administrators) to implement the cyber security program.
- Cyber security training is appropriate to the roles identified in the Senior DOE Management cyber security program.
- Increased awareness of cyber security concerns in the workplace.

Goal 4: Improve cyber security situational awareness

The complex and interdependent nature of the DOE's information systems and networks require shared cyber security awareness and understanding across the enterprise to enable effective operation. Senior DOE Management requires sufficient visibility into their network operations to ensure the security protections applied are appropriate to protect, defend, and respond to threats. To meet this need, the cyber security community must work to identify situational awareness requirements and build and deploy a performance measurement capability to fulfill these requirements.

Performance measurement, Figure 2, provides a clear and consistent way to measure success and demonstrate results for management. It helps to maintain a high-level overview of the current security posture by defining repeatable metrics and critical success factors.

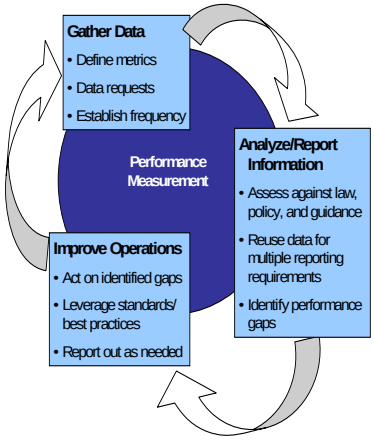


Figure 2. Performance Measurement

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 a feedback mechanism to adjust cyber security program and implementation, as needed. Performance measurement includes:

- Data Collection – Process for collecting and reporting cyber security metric information to provide all levels of the DOE with continuous status of the DOE's cyber security program.
- Metrics Development – Process to develop and maintain the criteria for effective evaluation of the cyber security program.
- Compliance and Monitoring Reviews – Process employed by the OCIO to review compliance with established policy and guidance.
- Compliance Reporting – Establishes the process of delivering a standard set of reports that documents the DOE's current cyber security posture and status of its FISMA milestones.
- Maturity Measurement – Process for evaluating all elements of the DOE's cyber security program to identify the overall maturity of the program elements and areas for process improvements.

Strategic Objective 4.1: Maintain a DOE-wide near-real-time cyber security operational picture

A cyber security operational picture of the networks, the missions these networks support, and network cyber security status, provides Senior DOE Management and their organizations with greater flexibility and reduces the risk of negative impacts resulting from unilateral, uncoordinated actions

Near-Term – Continue operation of existing capabilities, such as the Cyber Protection Program[3] (CPP) sensor grid, and expand sensor coverage as resources permit. Define requirements for, and begin implementation of, improved information sharing; attack, sense, and warning (AS&W) capability; analysis of anomaly and CPP sensor data; DOE-wide incident management; and operational cyber security picture of the DOE enterprise.

Elements

- Develop and publish guidance on performance metrics to be used by the DOE CIO to evaluate cyber security performance, including metrics for CPP, AS&W, and Continuous Asset Monitoring System (CAMS).
- Continue operation of the CPP enterprise sensor grid.

[3] The DOE OCIO and the Cyber Division in the DOE Office of Intelligence and Counterintelligence (IN/CN) jointly fund the CPP. CPP implements a program to detect and deter hostile activities directed at the DOE's information assets.

CPP supports the placement of sensors that generate summary and alert information about boundary-crossing Internet traffic at Senior DOE Management operating units. These sensors return data directly to the operating units for their internal analysis, and to the Data Distributor (DD)—a central distribution system that resides at Pacific Northwest National Laboratory (PNNL). Packet content is not retained or sent to the DD. The data is used at the operating units to compare with their sources to corroborate suspected incidents, and to perform forensics. The IN/CN's Operational Analysis Center (OAC) at PNNL and CIAC also uses the data. Each operating unit has control over which analysis center receives its data via an account on the sensors.

- Expand CPP coverage by adding additional sensors.
- Develop policies, processes, and procedures for information sharing from enterprise-wide CPP sensor capabilities.
- Define requirements for an AS&W capability and other anomaly detection and analysis capabilities for integration with CPP sensor and data collection capabilities.
- Enhance CPP sensors to handle additional performance needs.
- Develop and publish guidance for timely cyber incident reporting and notification processes for the DOE enterprise.
- Implement a DOE enterprise-wide incident management capability.
- Provide a cyber security operational picture of the DOE enterprise.
- Develop and publish policies and guidance for rapid dissemination of warning information within DOE.
- Establish active relationships with other governmental agencies and organizations to provide critical data interchange.

Mid-Term -- Continue operation of existing capabilities, such as the CPP sensor grid, and expand sensor coverage as resources permit. Continue implementation, and enhance where necessary and resources permit, of information sharing, attack, sense and warning capability, and timely analysis of anomaly and CPP sensor data; DOE-wide incident management, and an operational cyber security picture of the DOE enterprise.

Elements

- Continue operation of CPP and expand by adding additional sensors yearly.
- Improve, standardize, and integrate CPP, incident management, and enterprise Network Operations Center (NOC) operations.
- Enhance / extend policies, processes and procedures for information sharing from enterprise-wide CPP sensor capabilities
- Continue to deploy and improve the AS&W capability and other anomaly detection and analysis capabilities for integration with CPP sensor and data collection capabilities.
- Continue to deploy and enhance the DOE enterprise-wide incident management capability.
- Deploy a cyber security operational picture of the DOE enterprise to all appropriate levels of DOE management.
- Deploy communications capabilities for rapid dissemination of incident and warning information within DOE.
- Review and refine, and automate where possible, timely cyber incident reporting and warning procedures for the extended enterprise.
- Maintain and expand, as needed, active relationships with other governmental agencies and organizations to provide critical data interchange.

Long Term - Continue operation of existing capabilities, such as the CPP sensor grid, and expand sensor coverage as resources permit. Continue implementation, and enhance where necessary and resources permit, of information sharing, AS&W capability, and timely analysis of anomaly and CPP sensor data; DOE-wide

incident management; and an operational cyber security picture of the DOE enterprise. Secure operation of our computer systems and networks demands shared awareness and understanding across the enterprise.

Elements

- Continuous improvement of the CPP capability.
- Upgrade selected CPP sensors to handle additional performance needs.
- Continue to deploy and enhance the DOE enterprise-wide incident management capability.
- Continue collection, analysis, delivery, and enhancement of a cyber security operational picture for the DOE enterprise to all appropriate levels of DOE management.
- Continue operation and improve, as needed, communications capabilities for rapid dissemination of incident and warning information within DOE.
- Continuous improvement and integration of CPP, incident management, and enterprise NOC operations.
- Maintain and expand, as needed, active relationships with other governmental agencies and organizations to provide critical data interchange.

Success Measures

- Continued operation, expansion, and upgrade of CPP to protect at least 85% of all DOE computing assets.
- Implemented policies, processes and procedures for information sharing from enterprise-wide CPP sensors.
- Deployment of an AS&W capability
- Deployment of other anomaly detection and analysis capabilities to include at least CPP sensor and data collection capabilities.
- DOE enterprise-wide incident management capability fully operational.
- Delivery of a cyber security operational picture of the DOE enterprise to all appropriate levels of DOE management.
- Rapid dissemination of warning information within DOE.
- Automated cyber incident reporting and warning for the extended enterprise.
- Integrated CPP, incident management, and enterprise NOC operations deployed.
- Active relationships with other governmental agencies and organizations to provide critical data interchange.

Strategic Objective 4.2: Implement integrated enterprise-wide asset management capability

Near-Term — Implement corporate asset management capability for all unclassified computing resources throughout the DOE.

Elements

- Deploy asset management capability including configuration and patch management, vulnerability discovery and remediation, and asset discovery in all unclassified computing environments in all Senior DOE Management operating units.
- Deploy Senior DOE Management (where desired) corporate asset management capability to collect and integrate unclassified computing environment asset management information from operating units.
- Deploy DOE corporate asset management capability to collect and integrate unclassified computing environment asset management information from Senior DOE Management offices and operating units.
- Deploy an automated FISMA data collection and reporting capability.
- Define INFOCON processes for courses of action, reduction of decision and execution timelines, and evaluation of effects across the enterprise

Mid-Term — Implement corporate asset management capability for all national security computing resources throughout DOE.

Elements

- Deploy corporate asset management capability including configuration and patch management, vulnerability discovery and remediation, and asset discovery in all national security computing environments in all Senior DOE Management operating units.
- Deploy Senior DOE Management (where desired) corporate asset management capability to collect and integrate national security computing environment asset management information from operating units.
- Deploy DOE corporate asset management capability to collect and integrate national security computing environment asset management information from Senior DOE Management offices and operating units.
- Develop and publish guidance for INFOCON processes.
- Establish INFOCON modeling and simulation capabilities to better support courses of action, decision and execution timelines, and evaluation of effects across the enterprise.

Long Term — Fully deployed, real-time, automated, secure, DOE-wide information systems inventory capability deployed, tested, and verified.

Elements

- Upgrade, as needed, software licenses and hardware resources used to support corporate computing asset management throughout DOE.
- Develop and deploy additional asset management capabilities needed for new hardware or software products deployed within DOE.

- Improve INFOCON process and supporting modeling and simulation capabilities to better develop courses of action, reduce decision and execution timelines, and evaluate effects across the enterprise.

Success Measures

- Operational INFOCON processes.
- Fully integrated operations and corporate asset management capability.
- DOE-wide reporting of 100% of information systems inventory.
- Compliance with FISMA and OMB reporting requirements.