U.S DEPARTMENT OF ENERGY
ENTERPRISE ARCHITECTURE



IT SECURITY ARCHITECTURE

FEBRUARY 2007

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Background

The Department of Energy (DOE) EA Transition Plan (EATP) identifies, evaluates and sequences transition activities that will migrate DOE to its "To- Be" business and enabling information technology environments, as defined in the February 2007 DOE EATP. The purpose of establishing the DOE IT Security Architecture is to provide a holistic framework, based upon official DOE CIO Guidance, for the management of IT Security across DOE. The purpose of the DOE IT Security Architecture is to provide guidance that enables a secure operating environment. The architecture is driven by the Department's strategies and links IT security management business activities to those strategies.

The purpose of establishing the DOE IT Security Architecture is to provide a holistic framework for the management of IT Security across DOE. The DOE IT Security Architecture effort has been organized within this document based upon the OMB Security and Privacy Profile v2.0. The DOE IT Security Architecture approaches IT Security as a distinct set of business activities that support and enable the Department's mission functions. The DOE IT Security Architecture effort has been organized within this document based upon the OMB Security and Privacy Profile v2.0. In addition, the purpose of the DOE IT Security Architecture is to provide guidance that enables a secure operating environment. The architecture is driven by the Department's strategies and links IT security management business activities to those strategies.

The key to the cyber security program is identifying and documenting individual and organizational core values that ensure all levels of Federal and contractor personnel supporting the DOE behave in a manner that supports the strategic cyber security mission and goals. Fundamental to these core values are personal commitment, mutual trust, open communication, continuous improvement, and the full involvement of all affected parties. The core values of Teamwork, Integrity and Respect, Ownership and Accountability, Timeliness, and Honoring Our Partners provide the framework by which cyber security program concepts, technology, and guidance will be implemented to support the DOE community and their diverse missions.

1.2 Cyber Security Goals

1.2.1 Protect DOE information and information systems to ensure that the confidentiality, integrity, and availability of all information are protected 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. We can no longer rely simply on transport mechanisms/link encryption to provide our end-to-end protection. 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 physical or logical location. 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, achieving the goal of trusted 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, Departmental 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 Program Cyber Security Plans (PCSPs), Senior DOE Management implements the program defined in the policy and guidance for their organizations. The Departmental 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.

Achieving this goal of trusted 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.

[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

1.2.1.1 Strategic Objectives

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

- Strategic Objective 1.2: Provide policy and guidance adaptable to meet mission needs and aligned with the current threats.

- Strategic Objective 1.3: Protect information by recognizing and responding to threats, vulnerabilities, and deficiencies; ensuring that all systems and networks are capable of self-defense

- Strategic Objective 1.4: Establish and maintain a DOE enterprise cyber security architecture

1.2.2 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.

1.2.2.1 Strategic Objectives

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

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

1.2.3 Develop a cyber security empowered 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 understand their roles and responsibilities in protecting the Department’s information

assets and are prepared to react to today's and tomorrow's threats. In today's 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.

1.2.3.1 Strategic Objectives

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

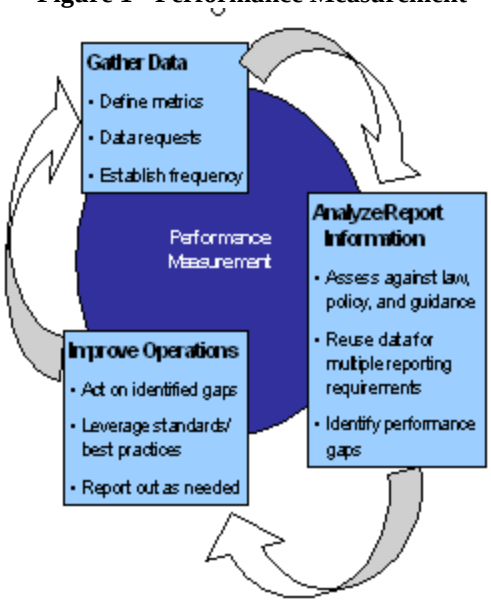
- Strategic Objective 3.2: Promote understanding and acceptance of cyber security principles throughout the DOE

1.2.4 Improve cyber security situational awareness

The complex and interdependent nature of the Department'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 1, 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. 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.

Figure 1 - Performance Measurement



Performance measurement includes:

- Data Collection – Process for collecting and reporting cyber security metric information to provide all levels of the Department with continuous status of the Department'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 Department's current cyber security posture and status of its FISMA milestones.
- Maturity Measurement – Process for evaluating all elements of the Department's cyber security program to identify the overall maturity of the program elements and areas for process improvements.

1.2.4.1 Strategic Objectives

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

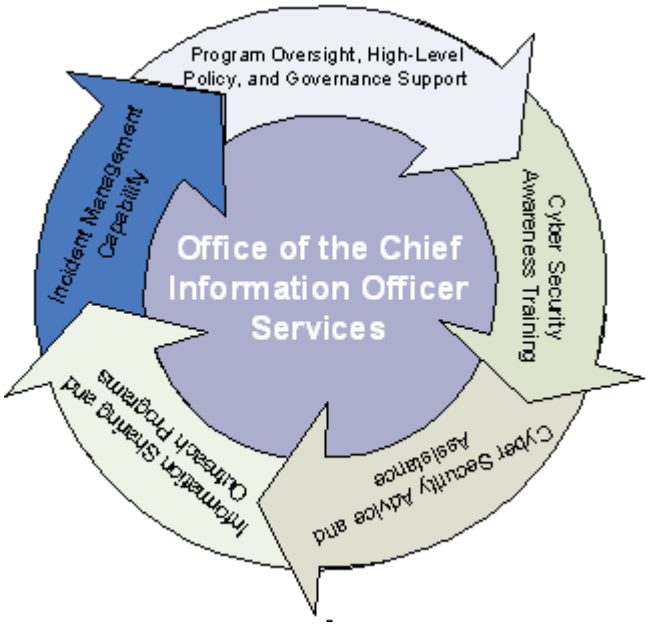
- Strategic Objective 4.2: Implement integrated enterprise-wide asset management capability

1.2.5 Provide DOE-wide cyber security services

The DOE cyber security program provides various services 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.

Figure 2 - CIO Services



1.2.5.1 Strategic Objective

- Strategic Objective 5.1: Implement DOE-wide cyber security services.

1.3 Intended Audience

- DOE Executives - 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 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. 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.

- Cyber Security Personnel - Focuses on Office of Cyber Security staff, but also includes all personnel responsible for managing the Department-wide cyber security programs that provides assistance and guidance in cyber security areas across all DOE entities.

- Network Managers - Network Managers have read access to network management reports, and do not have access to network devices.

- Network Operators - Network Operators have limited privileged access to network devices in order to facilitate troubleshooting activities.

- System Administrators - System Administrators have full privileged access to network devices.

- DOE Federal and Contractor Employees - This group, representing the network's primary customers at either the DOE HQ complex or at DOE field sites, exchanges corporate information in support of general management and administrative functions.

- Independent Auditors - Audit entities of the DOE organization (e.g., external third-party, DOE Inspector General) that would be responsible for conducting security audits or assessments on the DOE Infrastructure.

1.4 Legislative Drivers

- Clinger-Cohen Act of 1996 PL 104-106

- Freedom of Information Act (FOIA) and Amendments (5 USC § 552)

- Federal Information Security Management Act of 2002 (FISMA)
  - Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
  - FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems

- OMB Circulars A-130 and A-11

- Privacy Act (5 USC § 552a)

1.5 DOE Business Drivers

- Deputy Secretary's directive to remedy weaknesses in DOE's unclassified cyber security program, prompted by results of network penetration testing (red teaming) that exposed system vulnerabilities at DOE HQ and field organizations.

- February 2006 DOE Cyber Security Revitalization Plan, which aims to upgrade the DOE cyber security posture over the next year, and is designed to strengthen the Department's networks and establish a vital, institutionalized cyber security program.

- Compliance with FISMA mandated FIPS and NIST requirements that define protective measures and controls for certified and accredited applications (classified and non-classified) along with supporting technologies, business functions addressed by activity, and establish a level of "security due diligence" for the Department of Energy.

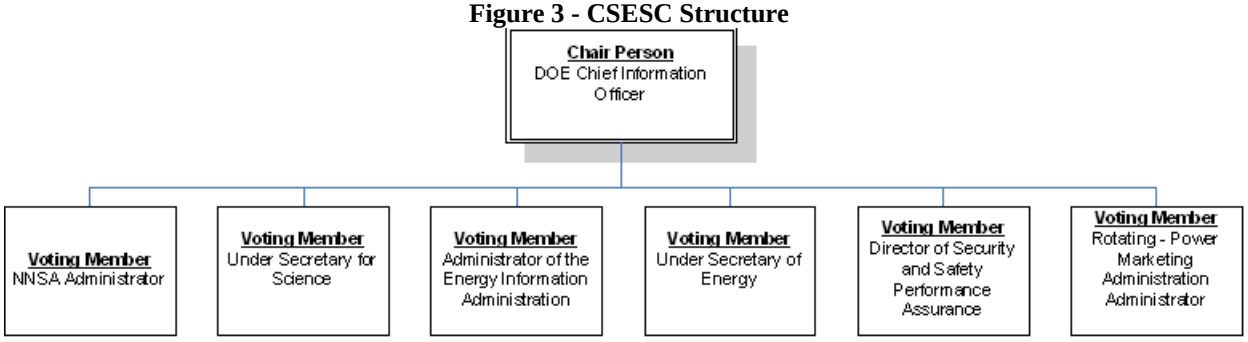
1.6 DOE Security Governance

1.6.1 Cyber Security Executive Steering Committee (CSESC)

The purpose of the CSESC is to provide advice and oversight for the cyber security program in the Department of Energy, including the National Nuclear Security Administration. The CSESC is charged with:

- Advise the Department of Energy Chief Information Officer (CIO) on cyber security issues within the Department, including development of a comprehensive, Department-wide cyber security program
- Provide oversight of the development of the comprehensive cyber security program and Department-wide implementation of it in a way that best supports the mission of each element of the Department.
- Serve as champions for the DOE cyber security program to ensure Department-wide support and prioritization.
- Leverage Departmental cyber security expertise in the Headquarters, programs, staff offices, and national laboratories, including the independent oversight function of the Office of Security and safety Performance Assurance.
- Meet quarterly, at a minimum, to review cyber security program cost, schedule and performance, and to address current cyber security issues.
- Identify resources adequate to implement the Department-wide cyber security program, working with the Chief Financial Officer
- Establish a Cyber Security Working Group to work with the CIO in planning the details of the Department-wide cyber security program and in coordinating its implementation

Figure 3 - CSESC Structure



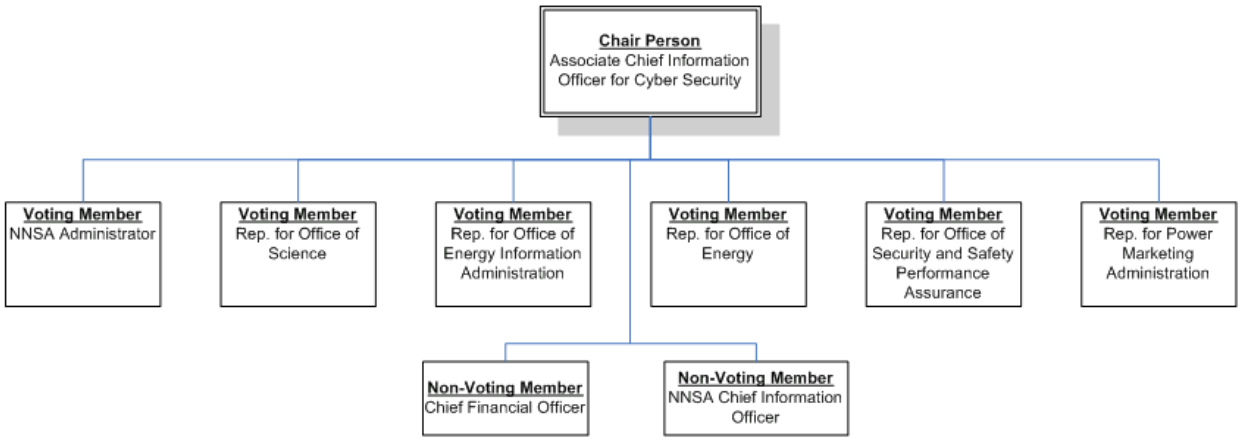
1.6.2 Cyber Security Working Group (CSWG)

The purpose of the CSWG is to manage the development of Departmental approaches, maintain compliance with national standards, and ensure adequate performance of the cyber security program at DOE, including the National Nuclear Security Administration (NNSA). The CSWG

serves as staff for Cyber Security Executive Steering Committee (CSESC) and supports action and coordination of the DOE cyber security program policy, technical, and operational activities. The CSWG is charged with:

- Advising the CSESC on cyber security issues and implement their decisions, coordinate DOE and NNSA, and program major initiatives, agree upon Departmental implementation patterns for cyber security, and ensure that cyber security is tailored to the needs of the missions.
- Provide strategic and tactical direction and support, and serve as architects of the DOE cyber security program to ensure effective Department-wide implementation and prioritization.
- Meet monthly, at a minimum, to develop cyber security program approaches and initiatives, monitor progress, cost, schedule and performance, and address current and evolving cyber security issues.
- Develop and monitor the implementation of prioritized plans of actions linked to resources and implementation schedules for the DOE cyber security program.
- Identify resource requirements adequate to implement the DOE, including NNSA, cyber security program.
- Enable threat mitigation best practices, incident reporting and analysis, and information sharing across the Department, including NNSA.
- Integrate and institutionalize the cyber security program with aligned resource planning and architectural processes and artifacts.
- Ensure that contractors and other interconnected organizations and entities implement adequate controls to safeguard DOE, including NNSA, information and information systems.
- Establish special interest task groups and task organizations within DOE and NNSA as needed to guide the development of the DOE/NNSA cyber security program. Each task groups or tasking supports the development, maintenance, and coordination of the DOE cyber security program policy, technical, and operational activities. These task groups will serve at the request of the CSWG, support their requests, and will be dissolved at the discretion of the CSWG.

Figure 4 - CSWG Structure



1.7 DOE Alignment with OMB Security & Privacy Profile v2.0

Figure 5 - Policy Alignment

OMB SPP v2.0 Requirements

OMB SPP v2.0 Requirements	CS-1	CS-2	CS-3	CS-4	CS-5	CS-6	CS-7	CS-12	CS-13	CS-14	CS-20	CS-38a
Access Control	√							√	√	√		√
Audit and Accountability	√										√	
System and Communications Protection	√								√			
Identification and Authentication	√							√				
Incident Response	√										√	√
System and Information Integrity	√				√				√			
Awareness and Training	√											
C&A and Security Assessments	√	√		√	√	√						
Configuration Management	√				√							
Contingency Planning	√						√					
Maintenance	√											
Media Protection	√											√
Personnel Security	√											
Physical and Environmental Protection	√											
Risk Assessment	√		√	√								
System and Services Acquisition	√											
System Security Planning	√											

2 Security Control Families

2.1 System and Information Integrity

2.1.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update System and Information Integrity policies, procedures, and practices that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document System and Information Integrity policies, practices, and processes and their associated System and Information Integrity controls for all information systems within their operating units.

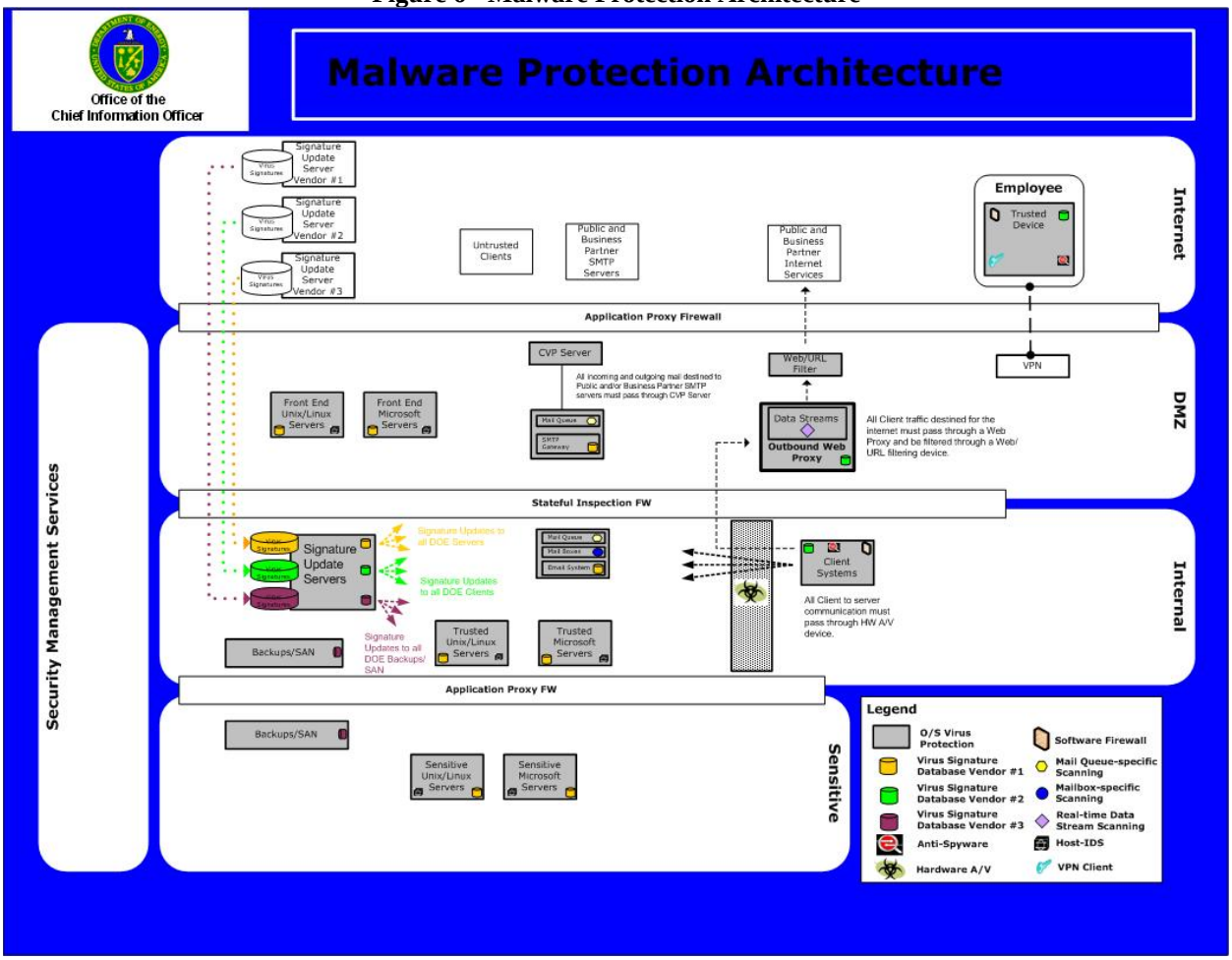
2.1.2 Malware Protection Architecture

With the evolution of the many variations of malicious code in the world today - it is not possible to prevent 100% of this code from reaching the Enterprise infrastructure. Instead, the goal must be to strive for 100%: identification, containment, isolation, and the prevention of any malicious content spreading through the enterprise. This can be accomplished by organizing the infrastructure into five unique areas of protection:

- Network
- Server
- Backups
- Client
- Email

Each area must have the capability to interrogate the data stream for malicious code within the commonly used internet applications of HyperText Transfer Protocol (HTTP), Secure HTTP (HTTPS), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP), and should be able to interrogate the data stream of the commonly used Microsoft communication ports.

Figure 6 - Malware Protection Architecture



2.1.2.1 Industry Trends

Four of the top ten security trends, from SANS, for 2007 revolve around malware…

- Cell phone worms - will infect at least 100,000 phones… That makes them fertile territory for attackers fueled by cell-phone adware profitability.
- Spyware - will continue to be a huge and growing issue. *The opportunity for profit drives spyware developers to open development and distribution centers throughout the developed and developing world.*
- Zero-day vulnerabilities - will result in major outbreaks resulting in many thousands of PCs being infected worldwide. Security vulnerability researchers often exploit the holes they discover before they sell them to vendors or vulnerability buyers like TippingPoint.
- BOTS with Rootkits - The majority of bots will be bundled with rootkits. The rootkits will change the operating system to hide the attack's presence and make uninstalling the malware almost impossible without reinstalling a clean operating system.[2]

[2] SANS (http://www.sans.org/resources/10_security_trends.pdf?ref=2411)

The US government and other nations are trying to do something about malware, including becoming party to the Council of Europe Convention on Cybercrime, which takes effect Jan 1, 2007…individuals and corporations must continue to educate themselves about the development of new malware threats in order to stay one step ahead of attackers. [3]

Five of the top ten security trends, from McAfee, for 2007 revolve around malware…

- Mobile phone attacks will become more prevalent as mobile devices become "smarter" and more connected
- Adware will go mainstream following the increase in commercial Potentially Unwanted Programs (PUPs)
- BOTS computer programs that perform automated tasks, will increase as a tool favored by hackers
- Parasitic malware/viruses that modify existing files on a disk, will make a comeback
- Rootkits - The number of rootkits on 32-bit platforms will increase, but protection and remediation capabilities will increase as well.[4]

2.1.2.2 Malware Guidance

National Institute of Standards and Technology (NIST):

- SP800-53 "Guide for Assessing the Security Controls in Federal Information Systems", Control SI-3 "Malicious Code Protection"
- SP800-83 "Guide to Malware Incident Prevention and Handling"

Office of Management and Budget (OMB):

- Circular A-130 "Management of Federal Information Resources", Appendix III "Security of Federal Automated Information Resources", Section 8.b(2)c(III) "Security Standards Profile"

Department of Energy Guidance:

- CIO Guidance CS-1, Control SI-3 "Malicious Code Protection"

2.1.2.3 Malware Protection Target Architecture

Applying the theory of "defense-in-depth" to the application layer is an efficient mechanism in protecting the enterprise against malicious code.

When protecting against malicious content, the same approach used in designing an infrastructure with multi-vendored firewalls must be applied in protection against malicious content; by utilizing multiple malware vendors in the fight against malicious content.

The Five areas of Malware Protection are:

- Network

[3] ITSecurity (http://www.itsecurity.com/features/nastiest-malware-trends-011207/)
[4] McAfee (http://www.mcafee.com/us/about/press/corporate/2006/20061129_080000_f.html)

- Server
- Backups
- Client
- Email

2.1.2.4 Network Component

The Network Components within the Malware Protection Architecture consist of Remote Access Devices, Web Proxy Servers, and a Hardware A/V Solution.

All Remote Access Devices must:

- Ensure that personnel that are permitted to gain access to the enterprise through the use of remote access have the appropriate:
    - Software Firewalls Enabled
    - Anti-Virus Software Enabled and signatures are up-to-date
    - Spyware Software Enabled and signatures are up-to-date

All Web Proxy Serves must:

- Ensure that all communication destined for the Internet must pass through a proxy device that is capable of scanning HTTP, HTTPS, FTP, POP3, and IMAP for malicious content.

It is typically very difficult to place a firewall between the user community and the various types of Microsoft servers in use within the enterprise. Even in an organization where the user community has been separated, by a firewall, from the Microsoft servers - the ports that are used to communicate between the client and server are typically the ones that malware use to spread their code. For this reason, a Hardware A/V solution is required. The Hardware A/V solution must be able to:

- Analyze all client to server communication must pass through a device that is capable of scanning HTTP, HTTPS, FTP, SMTP, POP3, IMAP, and be able to interrogate the data stream for the Microsoft communication ports.
- Isolate infected clients from communicating with other devices.
- Isolate unauthorized devices from communicating with authorized devices within the enterprise.
- Monitor clients in the enterprise to ensure that they are utilizing the most current signature files available. When devices that are not utilizing the most current signature files the appropriate update server must be notified and push the signature files to the out-of-date devices.

2.1.2.5 Server Component

To adequately protect the servers within the enterprise all servers must have an A/V solution and Host Intrusion Detection System installed. Not all A/V vendors are created equally – one vendor will always release a new signature to protect against the latest threats before another; therefore by aligning with the defense-in-depth approach to malware protection, all servers within the enterprise should have a different A/V solution than that of the clients.

2.1.2.6 Client Component

Given the number of different types of end users in a modern network environment, the user community presents perhaps the greatest level of challenge to secure. These users vary from VPN users, to contractors, to administrators; all having unique requirements. Therefore, all end user client machines must have the following software installed:

- Anti-Virus
- Anti-Spyware
- Software Firewall

These software applications are needed in order to maintain an efficient defense-in-depth strategy for the prevention of malicious content. The Anti-Virus and Anti-Spyware solutions require the least explanation as to why they are needed, due to common knowledge amongst the end-user community; however the Software Firewall is required in order to prevent unauthorized communication outbound from the client devices - it is common for certain types of malicious code to create communication streams in the background without the user's knowledge.

A hardware-based Anti-Virus solution must always remain in the communication path between the client and server. This not only helps protect the clients from receiving malicious code from an infected server on the network, or on the Internet, but more importantly it will help prevent a contractor or a non-approved device that is on the network from spreading malicious code.

2.1.2.7 Backups Component

In order to ensure the integrity of the organization's backup data, there must be a strategy for protecting backups from the infiltration of malicious content; otherwise data being restored might be corrupted or the organization could be re-infecting systems with malware during the restore process. Since the data being backed up is taken from the servers, it is recommended that the backup Anti-Virus solution be different than that of those deployed on the enterprise servers. By ensuring that all data is scanned for malicious content before it is written to the backup solution, the organization is ensuring the integrity of the data; should the disaster recovery plan need initiating.

2.1.2.8 Email Component

Email has become one of the most critical applications within the enterprise. It is also one of the methods most often utilized for transmitting malware. In the world of mobile devices, i.e. Blackberry's, PDA's , Pocket PC's, etc…, all inbound and outbound email communication must be scanned for malicious content.

2.1.2.9 Recommended Vendor Structure

The theory behind the vendor breakdown, shown below in Table 1, is to maximize the potential for the 100% identification, containment, isolation, and the prevention of any malicious content spreading through the enterprise.

- With the clients having the same vendor solution as the network it will maximize the potential for all clients having up-to-date signatures and not passing malicious code to the

enterprise servers. It is also easier to update a pass-through network device in real-time than it is to update thousands of client devices; so if an outbreak occurs the network solution has prevented the spread of the malicious code.

- With the servers having a different vendor from the clients it is not as likely that both the server and clients will become infected during the same outbreak of malicious code. One vendor always has the signatures available before the others.

Table 1 - Malware Vendor Breakdown

	Malware Vendor "A"	Malware Vendor "B"
Clients	X	
Servers		X
Network	X	
Email		X
Backups	X	

2.1.3 Flaw Remediation

The purpose for flaw remediation is to efficiently identify and correct information system flaws and share information on flaws identified with the DOE Cyber Incident Capability.

- For HIGH-impact information systems:
  - Centrally manage the flaw remediation process and install updates automatically without individual user intervention.
  - Employ automated mechanisms to periodically and, upon command, determine the state of information system components with regard to flaw remediation.

2.1.4 Intrusion Detection Tools and Techniques

The purpose for Intrusion Detection tools and techniques is to monitor events in near-real time so that DOE can detect/prevent attacks and provide identification of unauthorized use of the system.

All Senior DOE Management PCSPs must require Internet access points to have network-based intrusion detection systems and require all Internet-accessible operating unit web servers to have host-based intrusion detection systems in place and functioning.

- For HIGH-impact information systems, the Senior DOE Management PCSP should recommend:
  - Networking individual intrusion detection tools into a system-wide intrusion detection system using common protocols.
  - Employing automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
  - Employing automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling

reconfiguration of these mechanisms in support of attack isolation and elimination.

- Monitoring outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).

2.1.5 Alerts and Advisories

Receive cyber security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

- HIGH-impact information systems must make security alerts and advisories available throughout the organization as needed.

2.1.6 Security Function Verification

Information System Owners must document security functionality controls in their information systems security plans. All information systems must verify the correct operation of security functions, either upon system startup and restart, upon command by user with appropriate privilege, or at least quarterly;

All information systems must notify the system administrator upon system shutdown or restart when anomalies are discovered.

The Senior DOE Management PCSP should recommend, for HIGH-impact information systems:
Employment of automated mechanisms to provide notification of failed security tests.
Employment of automated mechanisms to support management of distributed security testing.

2.1.7 Software and Information Integrity

HIGH-impact information systems must detect and protect against unauthorized changes to software and information.

2.1.8 Information Input and Output

Information Input Restrictions:

- Restrict the information input to authorized personnel only for MODERATE- and HIGH-impact information systems.

Information Input Accuracy, Completeness, And Validity:

- MODERATE- and HIGH-impact information systems check information inputs for accuracy, completeness, and validity.

Error Handling:

- MODERATE- and HIGH-impact information systems identify and handle error conditions in an expeditious manner.

Information Output Handling And Retention:

- Handle and retain output from MODERATE- and HIGH-impact information systems in accordance with Departmental, Senior DOE Management, and operating unit policy and operational requirements.

2.2 Media Protection

2.2.1 Data Classifications

DOE utilizes the following data classifications:

- Public (FOIA) - This is publicly releasable material that would fall under the Freedom of Information Act (FOIA).
- For Official Use Only (FOUO)* - FOUO is applied to information that is unclassified yet exempt from release to the public under the Freedom of Information Act. In general, this information consists of sensitive administrative or personal information that warrants protection from unauthorized disclosure.
- Unclassified Controlled Nuclear* - UCNI is sensitive government information that is controlled even though it is not classified. A clearance is not required to view UNCI but a person must have a need to know. Security measures taken to protect UCNI transmissions must deter access by unauthorized individuals and restrict public release. UCNI must be protected by an approved encryption method when transmitted over public switched broadcast communications paths such as the Internet.
- Naval Nuclear Propulsion Information (NNPI)* - Defines information concerning the design, arrangement, development, manufacturing, testing, operation, administration, training, maintenance, and repair of the propulsion plants of Naval Nuclear Powered Ships including the associated shipboard and shore-based nuclear support facilities.
- Privacy Act Information* - This includes records on individuals that fall under the 1974 privacy act.
- Contractual Agreements* - Agreements between Department of Energy (DOE), NNSA, its contractors, and other entities such as commercial organizations or foreign governments
- Military / Dual Use Information* - This would include technologies on the Critical Infrastructure and Materials list identified by the Department of Defense (DOD)
- Non-Proliferation Information* - Unclassified sensitive data relating to nonproliferation efforts.
- Proprietary (Non-Third Party)* - The information was created within the DOE Enterprise and there exists ownership, control or use over an item of information. An example is intellectual property and business sensitive information created within the DOE Enterprise.
- Export-Controlled Information (ECI)* - The information falls under an Export Control Regulation and has restrictions for export to foreign countries.
- Proprietary Third Party (PTP) - Proprietary indicates that an external party the DOE Enterprise exercises private ownership, control or use over an item of information, usually to the exclusion of other parties. This would include external intellectual property as well as business sensitive information.

- Classified - This applies to data that would be below the Q level and would be on a general classified network.
- Classified National Security - Confidential or secret national security information
- Classified Restricted - confidential or secret restricted data - this is nuclear weapons data and is different from the other type of classified data.
- Special Access - This applies to data that is at a Q or higher levels. Typically this data is on a special access network
- HIPAA - The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191 incorporated provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.
- Supervisory Control and Data Acquisition (SCADA)

2.2.2 Data Confidentiality and Integrity

DOE provides data confidentiality mechanisms to protect sensitive data from inspection by unauthorized entities.

DOE provides data confidentially via approved FIPS140-2 compliant encryption algorithms for the following:

- All SBU data traveling over the Internet or other public network
- All SBU data traveling over a network leased for DOE use but not inside a DOE facility
- Sensitive data traveling over the DOE networks; i.e. financial or medical data - that should not be viewed by DOE personnel who have access to network resources; i.e. network operations personnel or network administrators.

2.3 Configuration Management

Configuration Management consists of:

- Identifying and controlling managed objects.
- An information database which defines all elements in the operational network and maintenance inventory.
    - Connectivity information
    - Equipment type or software release versions

- Configuration Management provides the capability and procedures to control the network by:
    - Initializing, operating, reconfiguring, and shutting down managed objects from a centralized network management workstation. The functional capabilities include the following:
        - Performing software verification checks of network entities;
        - Supporting deployment of new software and hardware in the networks;
        - Supporting network provisioning;
        - Providing database administration; and
        - Maintaining hardware, software, and firmware inventory.

2.4 Physical and Environmental Protection

2.4.1 Physical Security

- Physical access to network devices and servers can only be granted by the appropriate authority.
- Physical access is granted to personnel who have an operational or managerial need to access equipment.
- Equipment will be housed in limited access portions of the larger DOE facilities.
- Physical access to these zones should be restricted by locks or badge readers
- Contractors given physical access to DOE equipment must be escorted by a DOE employee with access to the equipment
- Foreign nationals should not be granted access to DOE equipment.

2.4.2 Environmental Protection

Power Equipment And Power Cabling:

- Protect power equipment and power cabling from damage and destruction for MODERATE- and HIGH-impact information systems.
- Senior DOE Management should consider recommending that each operating unit employ redundant and parallel power cabling paths for HIGH-impact information systems.

Emergency Shutoff:

- Provide the capability of shutting off power to any for MODERATE- and HIGH-impact information system component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.

Emergency Power:

- Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of MODERATE- and HIGH-impact information system in the event of a primary power source loss.
- Provide a long-term alternate power supply for HIGH-impact information systems that are capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
- Senior DOE Management should consider recommending that each operating unit provide a long-term alternate power supply for HIGH-impact information systems that is self-contained and not reliant on external power generation.

Emergency Lighting:

- Employ and maintain automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.

Fire Protection:

- Employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.
- Configure fire suppression and detection devices/systems to activate automatically in the event of a fire for MODERATE- and HIGH-impact information systems.
- Configure fire suppression and detection devices/systems to provide automatic notification of any activation to the organization and emergency responders for HIGH-impact information systems.

Temperature And Humidity Controls:

- Regularly maintain within acceptable levels and monitor the temperature and humidity within facilities containing information systems.

Water Damage Protection:

- Protect the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.
- Employ automated mechanisms to automatically close shutoff valves in the event of a significant water leak for HIGH-impact information systems.

Delivery And Removal:

- Control information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintain appropriate records of those items.

Alternate Work Site:

- Require that individuals within the operating unit employ appropriate cyber security controls at alternate work sites for MODERATE- and HIGH-impact information systems.

2.5 Incident Response

DOE continues to operate with the ability to detect, analyze, contain, respond to, and recover from network-related events that could have a negative impact on a DOE computer or network operations. Those events, referred to as incidents, include the introduction of malicious code into the DOE environment, network-based attacks aimed at denying or degrading DOE network operations, and incidents of unauthorized access or unauthorized usage.

The DOE OCIO is responsible for managing the DOE-wide incident reporting and response. Part of that capability is the Computer Incident Advisory Capability, which provides warnings, analysis, and assistance to the general DOE user population regarding computer incidents.

DOE uses the Computer Security Incident Response Center, currently managed by the HQ Cyber Security Division, to provide the incident detection and response capabilities mentioned above. The CIAC is the focal point for coordinating security advisories from FedCIRC and CERT.

CIAC has the ability to gather and analyze data from:

- Network devices, including firewall, routers, and IDS, resident on DOE networks.

- DOE sites which send logs or other data relevant to DOE networks.
- Contracted service providers, such as ISPs
- CIAC also reports on incidents as outlined in the Headquarter Program Cyber Security Plan.

All service contracts, such as one between DOE and an ISP, have contract language to ensure:
Event data can be exchanged between the service provider and DOE operations.
Course of action in the event of service disruption or cessation by the provider.

2.6 Identification and Authentication

2.6.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update Identification and Authentication policies, procedures, and practices that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document Identification and Authentication policies, practices, and processes and their Identification and Authentication controls for all information systems within their operating units.

All information systems require:

- Distinct user IDs that are unique to each user or group for user identification
- All information systems require a user authentication mechanism that is unique to each user for primary access to all information and information system resources
- All information systems and associated equipment that rely on passwords as the means to authenticate users must implement effective password management in accordance with DOE CIO Guidance CS-12, Password Management

2.6.2 Identification and Authentication

User Identification And Authentication:

- Uniquely identify and authenticate users (or processes acting on behalf of users) on all information systems.
- For HIGH-impact information systems, employ multifactor authentication.

Device Identification And Authentication:

- For MODERATE and HIGH-impact information systems, identify and authenticate specific devices before establishing a connection.

2.6.3 Identification Management

Manage user identifiers by:

- Uniquely identifying each user
- Verifying the identity of each user
- Receiving authorization to issue a user identifier from an appropriate organization official
- Ensuring that the user identifier is issued to the intended party
- Disabling user identifier after a reasonable period of inactivity as documented by the operating unit in its procedures
- Archiving user identifier.

2.6.4 Authentication Management

Manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by:

- Defining initial authenticator content
- Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators
- Changing default authenticators upon information system installation.
- Electronic authentication methods to provide services to citizens must comply with OMB Memorandum 04-04, E-Authentication Guidance, and associated implementation requirements in NIST SP 800-63, Electronic Authentication Guideline.

2.6.5 Encryption

All information systems, requiring authentication, must ensure that the authentication credentials are encrypted using approved cryptographic modules that are compliant with FIPS 140-2.

2.6.6 Homeland Security Presidential Directive 12 (HSPD-12)

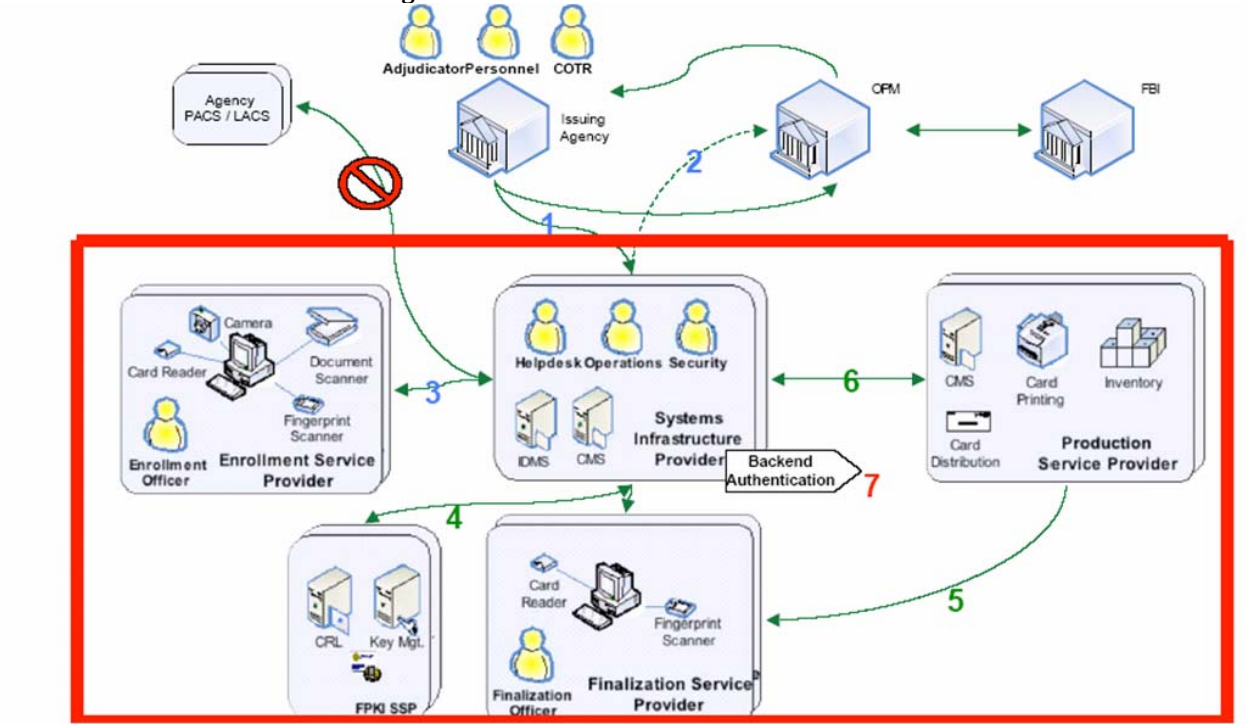
HSPD-12 was issued by the White House to establish more uniform standards for issuing government identity credentials. HSPD-12 will apply to all government employees and contractors and governs physical (facility) and logical (systems) access.

DOE utilizes Entrust Public Key Infrastructure (PKI), based on the X.509 framework to support the current infrastructure and plan for the implementation of HSPD-12. The DOE PKI infrastructure provides:

- Public key certificates
- Certificate repository
- Certificate revocation
- Key backup and recovery
- Support for non-repudiation of digital signatures
- Automatic update of key pairs and certificates

- Management of key histories
- Support for cross-certification
- Client-side software interacting with all of the above in a secure, consistent, and trustworthy manner.

Figure 7 - HSPD-12 Overview Architecture



2.7 Risk Assessment

2.7.1 Risk Management

DOE's risk management philosophy is composed of four distinct areas:

- Assessment
- Mitigation
- Evaluation
- Continuous assessment

Each area of the DOE Risk Management philosophy requires a cost-effective structured process for:

- Identifying
- Analyzing; and
- Reducing the potential impact of risk events

2.7.2 Risk Management Process

The DOE Risk management philosophy is applicable to all systems regardless of their stage in the system life cycle.

A uniform risk management process permits managers to:

- Effectively secure DOE general support systems (GSSs) and major applications (MAs)
- Make informed risk management decisions and focus information technology expenditures on mitigating current risk factors
- Ensure interoperability and portability
- Understand total operational and residual risk.

This approach includes:

- Identifying system and environmental threats and vulnerabilities
- Documenting decisions on the adequacy and maintenance of security controls
- Determining cost implications of enhanced protection
- Accepting residual risk
- Providing continuous monitoring of the system and environment to ensure that controls are performing as required and changes in network, physical security, and/or operations do not have an adverse impact on the system.

2.7.3 Risk Analysis

The major activities for conducting risk management analysis include:

- Risk Assessment:
  - Identify and describe each organizational system
  - Assess threats, vulnerabilities, likelihood of adverse actions, and potential consequences
  - Quantify the level(s) of risk based on the assessment
  - Develop a set of security controls based on the level(s) of risk
  - Document decisions made during the assessment

- Risk Mitigation:
  - Evaluate security controls and select those that provide the greatest level of risk reduction at the lowest cost
  - Identify appropriate security controls and assign responsibility to those individuals who will implement and maintain those controls
  - Implement security controls and document the implementation to provide input to the configuration baseline.

- Evaluation and Assessment:
  - The first two activities (risk assessment and risk mitigation) are properly documented and reflected in the system baseline
  - Security controls are implemented

2.8 Security Planning

2.8.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update Security Planning policies, procedures, and practices that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document Security Planning policies, practices, and processes and their associated Security Planning controls for all information systems within their operating units.

2.8.2 System Security Planning and Updates

System Security Plan:

- Develop and implement a security plan for each information system that provides an overview of:
  - Security requirements for the system
  - Description of the security controls in place or planned for meeting those requirements
  - Designated officials within the organization review and approve the plan.
- System Security Plan Update:
  - Define and document procedures to require a review of each system security plan, at least annually, as part of system self-assessments and to revise the plan to address significant changes and problems identified during plan implementation or security control assessments

2.8.3 Rules of Behavior

Establish and make readily available to all information system users a set of rules that describes:

- Responsibilities and expected behavior with regard to information system usage

The organization receives signed acknowledgement from users indicating they have:

- Read
- Understand, and;
- Agree to abide by the rules of behavior, including consent to monitoring, before authorizing access to the information system.

2.8.4 Privacy Impact Assessment

All Information System Owners must conduct a privacy impact assessment on applicable information systems, as defined in the PCSP.

2.9 System and Services Acquisition

2.9.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update System and Services Acquisition policies, procedures, and practices that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document System and Services Acquisition policies, practices, and processes and their associated System and Services Acquisition controls for all information systems within their operating units

2.9.2 System and Services Acquisition

Allocation of Resources:

- Determine, document, and allocate as part of its capital planning and investment control process the resources required to adequately protect the information system.

Life Cycle Support:

- Manage information systems using a system development life cycle methodology that includes information security considerations.

Acquisitions:

- Include security requirements and/or security specifications, either explicitly or by reference, in information system and information technology service acquisition contracts based on an assessment of risk.

2.9.3 Information System Documentation

Ensure that adequate documentation for their information systems and constituent components is available, protected when required, and distributed to authorized personnel.

- Document the functional properties of the security controls employed within MODERATE and HIGH-impact systems with sufficient detail to permit analysis and testing of the controls is available.

- Document the design and implementation details of the security controls employed within HIGH-impact information systems with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components) is available.

2.9.4 Software

Software Usage Restrictions:

- Comply with software usage restrictions established in the Senior DOE Management PCSP.

User Installed Software:

- Enforce explicit rules governing the downloading and installation of external software by users.

2.9.5 Security Design Principles

Senior DOE Management should consider recommending that each operating unit design and implement information systems using the security engineering principles as recommended in NIST SP 800-27A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security) Revision A.*

2.9.6 Outsourced Information System Services

Senior DOE Management PCSPs are to require each operating unit to monitor security control compliance from outsourced services.

Senior DOE Management must ensure that third-party providers of information system services employ adequate security controls in accordance with:

- Federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.

2.9.7 Developer Security Testing

All information systems must create a security test and evaluation plan. The security test and evaluation plan must be executed, at a minimum, on an annual basis. The results of the plan need to be used in support of the C&A process.

2.10 Certification and Accreditation

2.10.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update C&A policies, procedures, and practices that address:

- Purpose
- Scope
- Roles

- Responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document the security assessment and certification and accreditation policies, practices, and processes and their associated assessment, certification, and accreditation controls for all information systems within their operating units.

2.10.2 Security Assessments

All information systems must conduct security assessments, based upon their DOE Operating Unit's PCSP, that test the effectiveness of security controls in each information system, at least annually**,** to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome in meeting the security requirements for the system.

2.10.3 Information System Connections

All information systems must explicitly authorize all connections to an information system from outside of the accreditation boundary and monitor/control the system interconnections on an ongoing basis.

2.10.4 Certification and Accreditation

All information systems must perform an assessment of the security controls within the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

All information systems must receive an authorization to operate (ATO) and update the authorization must be updated, at a minimum, every 3 years or upon significant change to the system.

2.10.5 POA&M

All Information System Owners must develop and update, according to the frequency specified in the PCSP, a plan of action and milestones (POA&M) for its information systems that 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 system.

2.10.6 Continuous Monitoring

All information systems must be continuously monitored for effectiveness and adequacy of system controls in accordance with the Senior DOE Management PCSP.

2.11 Personnel Security

2.11.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update Personnel Security policies, procedures, and practices that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document Personnel Security policies, practices, and processes and their associated Personnel Security controls for all information systems within their operating units.

2.11.2 Position Categorization

Senior DOE Management must be assign a risk designation to all positions and establish screening criteria for individuals filling those positions.

The Senior DOE Management operating unit Chief Information Officer (or equivalent), in coordination with the operating unit's Office of Human Resources, Office of Security, and Office of Acquisition Management reviews and revises position risk designations on a sampling basis, at a minimum of every three years.

2.11.3 Personnel Screening

Senior DOE Management must require that all personnel, where applicable, be subject to the screening process prior to being permitted permanent access to information and information system resources.

Screening must be performed for operating unit employees, contractors, and any "guests" prior to their being given access to operating unit systems and networks.

A risk-based, cost-effective approach must be followed to determine the risk of harm to the system in comparison to the opportunity for personnel performing the following functions:

- Personnel with cyber security authority, "root" access to systems, or access to software source code who have opportunity to bypass system security control settings – for example, network/system administrator,
- System developer, and cyber security program positions (such as ISSOs and cyber security managers).

- User with root access to MODERATE- OR HIGH-impact information systems who may modify core data stores, users with authority to electronically approve financial transactions, or users with access to personal/Privacy Act/other protected data (e.g., social security numbers in human resource systems, etc.) other than their own.
- Users with access to an operating unit local area network, e-mail, basic office applications (such as Microsoft Office or Corel Office suites), and personal data records (i.e., only personal/private information pertaining to themselves such as their personal time and attendance record or Thrift Savings Plan account).

2.11.4 Changes in Personnel

Personnel Termination:

- When employment is terminated the following actions must occur according to the organization unit's PCSP:
  - Terminate user information system access
  - Conduct exit interviews
  - Ensure the return all organizational information system-related property (e.g., keys, identification cards, building passes) in a timely manner.
  - Appropriate personnel are to be granted access to all official records created by the terminated employee that are stored on organizational information systems before the systems are recycled or disposed.

Personnel Transfer:

- Review information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).

2.11.5 Access Agreements

Complete appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for all individuals requiring access to organizational information and information systems before authorizing access.

2.11.6 Third Party Personnel Security

Comply with the personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) established by Senior DOE Management PCSP and monitor provider compliance to ensure adequate security.

2.11.7 Personnel Sanctions

Comply with the formal sanctions process for personnel failing to comply with established information security policies and procedures established by the Senior DOE Management PCSP.

2.12 Contingency Planning

2.12.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update Contingency Planning policies, procedures, and practices that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document Contingency Planning policies, practices, and processes and their associated Contingency Planning controls for all information systems within their operating units.

2.12.2 Contingency Plan

All Information System Owners must develop and implement a contingency plan for each information system addressing:

- Contingency roles
- Responsibilities
- Assigned individuals with contact information
- Activities associated with restoring the system after a disruption or failure.

Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

2.12.3 Training

All DOE personnel having roles relating to contingency planning must be trained in their contingency roles and responsibilities.

All DOE personnel having contingency roles and responsibilities relating to MODERATE- and HIGH-impact information systems and must be provided refresher training, at a minimum, on an annual basis. This training must:

- Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations for HIGH-impact information systems.
- Use of automated mechanisms is recommended to provide a more thorough and realistic training environment.

2.12.4 Testing

Contingency plans for MODERATE- and HIGH-impact information systems must be tested, at a minimum, on an annual basis, using operating unit-defined tests and exercises to determine the

plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the operating units review the contingency plan test results and initiate corrective actions.

Information System Owners must coordinate contingency plan testing for MODERATE- and HIGH-impact information systems with organizational operating units responsible for:

- Related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
- Test the contingency plan for HIGH-impact information systems at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.
- For HIGH-impact information systems, the use of automated mechanisms to more thoroughly and effectively test the contingency plan is recommended.

2.12.5 Plan Updates

All information systems must review their contingency plan, at a minimum, on an annual basis and revise the plan to address:

- System/organizational changes
- Problems encountered during plan implementation
- Execution
- Testing

2.12.6 Alternate Sites

Alternate Storage Sites:

- Identify an alternate storage site and initiate necessary agreements to permit the storage of MODERATE- and HIGH-impact information systems backup information.
- For MODERATE- and HIGH-impact information systems, geographically separate alternate storage site(s) from the primary storage site so as not to be susceptible to the same hazards.
- For HIGH-impact information systems, configure alternate storage site(s) to facilitate timely and effective recovery operations and the operating units identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Alternate Processing Sites:

- Identify an alternate processing site and initiate necessary agreements to permit the resumption of MODERATE- and HIGH-impact information systems operations for critical mission/business functions in a timely manner, as specified by the operating units in the information system SSP when the primary processing capabilities are unavailable.
- For MODERATE- and HIGH-impact information systems:
    - Geographically separate Alternate processing site(s) are from the primary processing site so as not to be susceptible to the same hazards;

    - Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions; and
    - Include priority-of-service provisions in alternate processing site agreements in accordance with the organization's availability requirements.
- For HIGH-impact information systems, configure alternate processing site(s) to fully support a minimum required operational capability and be ready to use as the operational site.

2.12.7 Telecommunication Services

Identify primary and alternate telecommunications services to support MODERATE- and HIGH-impact information systems and initiate necessary agreements to permit the resumption of MODERATE- and HIGH-impact information systems operations for critical mission/business functions in a timely manner, as specified by the operating unit when the primary telecommunications capabilities are unavailable.
For MODERATE and HIGH-impact information systems:

- Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.
- Alternate telecommunications services do not share a single point of failure with primary telecommunications services.

For HIGH-impact information systems:

- Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.
- Primary and alternate telecommunications service providers have adequate contingency plans.

2.12.8 Backup, Recovery, and Reconstitution

Information System Backup:

- Conduct backups of user-level and system-level information (including system state information) contained in the information system, at a minimum, on an annual basis and stores backup information at an appropriately secured location.
    - Test backup information for MODERATE- and HIGH-impact information systems, at a minimum, on an annual basis to ensure media reliability and information integrity.
    - For HIGH-impact information systems:
        - Selective use of backup information in the restoration of information system functions as part of contingency plan testing.
        - Storing of backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

Information System Recovery and Reconstitution:

- Employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.
    - Include a full recovery and reconstitution of HIGH-impact information systems as part of contingency plan testing.

2.13 Maintenance

2.13.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update Maintenance policies, procedures, and practices that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document Maintenance policies, practices, and processes and their associated Maintenance controls for all information systems within their operating units.

2.13.2 Periodic Maintenance

Schedule, perform, and document routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or operating unit requirements.

Maintain a maintenance log for MODERATE- and HIGH-impact information systems that includes:

- Date and time of maintenance
- Name of the individual performing the maintenance
- Name of escort, if necessary
- Description of the maintenance performed
- List of equipment removed or replaced (including identification numbers, if applicable).

Employ automated mechanisms to ensure that periodic maintenance for HIGH-impact information systems is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.

2.13.3 Maintenance Tools

Approve, control, and monitor the use of MODERATE- and HIGH-impact information systems maintenance tools and maintain the tools on an ongoing basis.

For HIGH-impact information systems:

- Inspect all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.
- Check all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.
- Check all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.
- Employ automated mechanisms to ensure only authorized personnel use maintenance tools.

2.13.4 Remote Maintenance

Approve, control, and monitor remotely executed maintenance and diagnostic activities.

For HIGH-impact information systems:

- Audit all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.
- Address the installation and use of remote diagnostic links in the system security plan for the information system.
- Remote diagnostic or maintenance services are acceptable if performed by a service or operating unit that implements for its own information system the same level of security as that implemented on the information system being serviced.

2.13.5 Maintenance Personnel

Only authorized personnel are permitted to perform maintenance on information systems. A list of personnel authorized to perform maintenance on the information system should be maintained and kept up to date.

2.13.6 Timely Maintenance

Obtain maintenance support and spare parts for key MODERATE- and HIGH-impact information systems components within a time frame to support mission requirement following a failure.

2.14 Awareness and Training

2.14.1 Policy and Procedures

Each Senior DOE Management organization is responsible for developing, disseminating, periodically reviewing, and updating:

- Formal awareness and training policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- Formal documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls for all information systems in all Senior DOE Management operating units

2.14.2 Awareness

Senior DOE Management will provide all users, both DOE employees and contractors, basic cyber security awareness instruction within 30 days of appointment and before granting permanent access to any DOE System. Senior DOE Management will provide all DOE users, both DOE employees and contractors, cyber security awareness instruction on an annual basis. Cyber Security training will present a core set of generic cyber security terms and concepts for all personnel as a baseline for role-based learning, expands on those basic concepts, and provides a mechanism for students to relate and apply the information learned on the job.

2.14.3 Security Training and Records

Identify personnel with significant cyber security roles and responsibilities, document those roles and responsibilities, and provide appropriate cyber security training before authorizing access to the system. Establish, and, at least bi-annually, execute training plans for these personnel covering the training topics. Document and monitor individual cyber security training activities, including basic security awareness training and specific cyber security training.

2.15 Access Control

2.15.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update Access Control policies that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document Access Control procedures, within their PCSP, and associated Access Control controls for all information systems within their operating units.

2.15.2 Account Management

Manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts and document the procedures for managing the accounts.

For MODERATE- and HIGH-impact systems:

- Employ automated mechanisms to support the management of information system accounts.
- Automatically terminate temporary and emergency accounts after a reasonable period as specified by the Senior DOE Management PCSP.
- Automatically disable inactive accounts after reasonable period as specified by the Senior DOE Management PCSP.

Employ automated mechanisms for HIGH-impact information systems account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.

2.15.3 Access Enforcement

Enforce assigned authorizations for controlling access to the information system in accordance with applicable policy.

For MODERATE and HIGH-impact systems, access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).

2.15.4 Information Flow Enforcement

For MODERATE- and HIGH-impact information systems, enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

2.15.5 Separation of Duties

For MODERATE- and HIGH-impact information systems, enforce separation of duties through assigned access authorizations.

2.15.6 Least Privilege

For MODERATE- and HIGH-impact information systems, enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

2.15.7 Unsuccessful Login Attempts

Document in information system SSPs and enforce a limit of, PCSP specified number, consecutive invalid access attempts by a user during an operating unit specified time period. The information system automatically locks the account/node for a time period defined by the operating unit or delays next login prompt according to a specified algorithm when the maximum number of unsuccessful attempts is exceeded.

For HIGH-impact systems, automatically lock the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

2.15.8 System Use Notification

Display an approved system-use notification message before granting system access informing potential users:

- The user is accessing a U.S. Government information system
- System usage may be monitored, recorded, and subject to audit
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties
- Use of the system indicates consent to monitoring and recording.
- System use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

All Information Systems must display the following warning banner (or close approximation) at login and require users to electronically acknowledge the warning (such as clicking on “OK” or “I agree” button to proceed):

> **WARNING**WARNING**WARNING**WARNING**WARNING**
> This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY.
> **WARNING**WARNING**WARNING**WARNING**WARNING**

2.15.9 Concurrent Session Control

For HIGH-impact information systems, limit the number of concurrent sessions for any user as defined in the information system SSP.

2.15.10 Session Lock

For MODERATE- and HIGH-impact information systems, prevent further access to the information system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

2.15.11 Session Termination

For MODERATE- and HIGH-impact information systems, automatically terminate a session after a period of inactivity specified in the information system SSP.

2.15.12 Supervise and Review

Supervise and review the activities of users with respect to the enforcement and usage of information system access controls.

Employ automated mechanisms to facilitate the review of user activities for HIGH-impact information systems.

2.15.13 Permitted Actions without Identification or Authentication

Identify specific user actions that can be performed on the information system without identification or authentication.

For MODERATE- and HIGH-impact information systems, permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

2.15.14 Automated Marking

For HIGH-impact information systems, mark output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

2.15.15 Remote Access

Document, monitor, and control all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

For MODERATE and HIGH-impact systems:

- Employ automated mechanisms to facilitate the monitoring and control of remote access methods.
- Use encryption to protect the confidentiality of remote access sessions.
- Control all remote accesses through a managed access control point.

2.15.16 Wireless

Establish usage restrictions and implementation guidance for wireless technologies; and document, monitor, and control wireless access to the information system. Appropriate

organizational officials authorize the use of wireless technologies. Use authentication and encryption to protect wireless access to MODERATE and HIGH-impact systems.

2.15.17 Portable and Mobile Devices

Establish usage restrictions and implementation guidance for portable and mobile devices. Document, monitor, and control device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices. Employ removable hard drives or cryptography to protect information residing on MODERATE and HIGH-impact system portable and mobile devices.

Senior DOE Management must create policies and procedures for the protection of portable/mobile devices that may currently or in the future contain potentially sensitive but unclassified data and/or personally identifiable information. The data that is being stored

2.15.18 Personally Owned Information Systems

Restrict the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of Federal information.

2.16 Audit and Accountability

2.16.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update Audit and Accountability policies that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document audit and accountability procedures, within their PCSP, and associated audit and accountability controls for all information systems within their operating units.

2.16.2 Auditable Events

All systems must have documented, within each information systems' SSP, which events generate auditable records:

- At a minimum, All High-Impact Information Systems must:
    - Compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.

- Manage the selection of events to be audited by individual components of the system.

- At a minimum, all Moderate-Impact Information Systems must:
  - Periodically review and update the list of information system-defined auditable events

2.16.3 Content of Audit Records

All systems must have documented, within each information systems' SSP, what the content of each auditable records contains. All Audit records must:

- Capture sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.
  - For MODERATE and HIGH-impact information systems, provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
  - For HIGH-impact information systems, provide the capability to centrally manage the content of audit records generated by individual components throughout the system.

2.16.4 Storage Capacity and Retention

All information systems must allocate sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded. Each information systems must have the configurations documented within their SSP.

All information systems must retain audit logs for a time period, which is specified in the information system SSP, and is consistent with Departmental and National Archives and Records Administration retention periods to provide support for after-the-fact investigations of security incidents and meet regulatory and organizational information retention requirements.

2.16.5 Processing, Monitoring, Analysis, and Reporting

In the event of an audit failure or audit storage capacity being reached, all information systems will alert appropriate organizational officials and take the appropriate actions specified by the information system SSP (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)

Regularly review/analyze audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

Employ automated mechanisms for HIGH-impact information systems to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Employ automated mechanisms for HIGH-impact information systems to immediately alert security personnel of inappropriate or unusual activities with security implications.

2.16.6 Reduction and Report Generation

Provide an audit reduction and report generation capability for each information system. HIGH-impact information systems, provide the capability to automatically process audit records for events of interest based upon selectable, event criteria.

2.16.7 Time Stamps

All Moderate and High impact systems must provide time stamps for use in audit record generation.

2.16.8 Protection of Audit Records

All information systems must employ mechanisms that protect system audit information and audit tools from unauthorized access, modification, and deletion.

2.17 System and Communications Protection

2.17.1 Policy and Procedures

All Senior DOE Management organizations must develop, and document within its PCSP, disseminate, and periodically review and update System and Communication Protection policies that address:

- Purpose
- Scope
- Roles
- Responsibilities
- Management Commitment
- Coordination among organizational entities
- Compliance

All Senior DOE Management organizations must document System and Communication Protection procedures, within their PCSP, and associated System and Communication Protection controls for all information systems within their operating units.

2.17.2 Application Partitioning

For MODERATE- and HIGH-impact information systems, separate user functionality (including user interface services) from information system management functionality.

2.17.3 Security Function Isolation

For HIGH-impact systems:

- Isolate security functions from non-security functions by means of:
    - Partitions
    - Domains
    - Control access and integrity to the security functions of:
        - Hardware
        - Software

        - Firmware
    - The information system must maintain a separate execution domain (e.g., address space) for each executing process.

2.17.4 Information Remnants

For MODERATE- and HIGH-impact information systems:

- Prevent unauthorized and unintended information transfer via shared system resources.

2.17.5 Denial of Service Protection

Protect against or limit the effects of denial of service attacks listed in the information system SSP for all information systems.

All information systems should:

- Restrict the ability of users to launch denial of service attacks against other information systems or networks.
- Manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

2.17.6 Resource Priority

For MODERATE- and HIGH-impact information systems, limit the use of resources by priority.

2.17.7 Boundary Protection

Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. Physically allocate publicly accessible MODERATE- and HIGH-impact information systems components (e.g., public web servers) to separate sub-networks with separate, physical network interfaces.

2.17.8 Transmission Integrity

For MODERATE- and HIGH-impact information systems, protect the integrity of transmitted information. Employ cryptographic mechanisms for HIGH-impact information systems to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).

2.17.9 Transmission Confidentiality

For MODERATE- and HIGH-impact information systems, protect the confidentiality of transmitted information. Employ cryptographic mechanisms for HIGH-impact information systems to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).

2.17.10 Network Disconnect

For MODERATE- and HIGH-impact information systems, terminate a network connection at the end of a session or [after a time specified in the information system SSP

2.17.11 Cryptography

Cryptographic Key Establishment and Management:

- Employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management for MODERATE- and HIGH-impact information systems.

Use Of Validated Cryptography:

- When cryptography is employed within the information system, perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

2.17.12 Public Access Protections

For publicly available systems, protect the integrity of the information and applications as stated within the information systems SSP.

2.17.13 Collaborative Computing

For MODERATE- and HIGH-impact information systems, prohibit remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provide an explicit indication of use to the local users (e.g., use of camera or microphone).

2.17.14 PKI

Develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in MODERATE- and HIGH-impact systems.

2.17.15 Mobile Code

For MODERATE- and HIGH-impact systems:

- Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously Document, monitor, and control the use of mobile code within the information system.

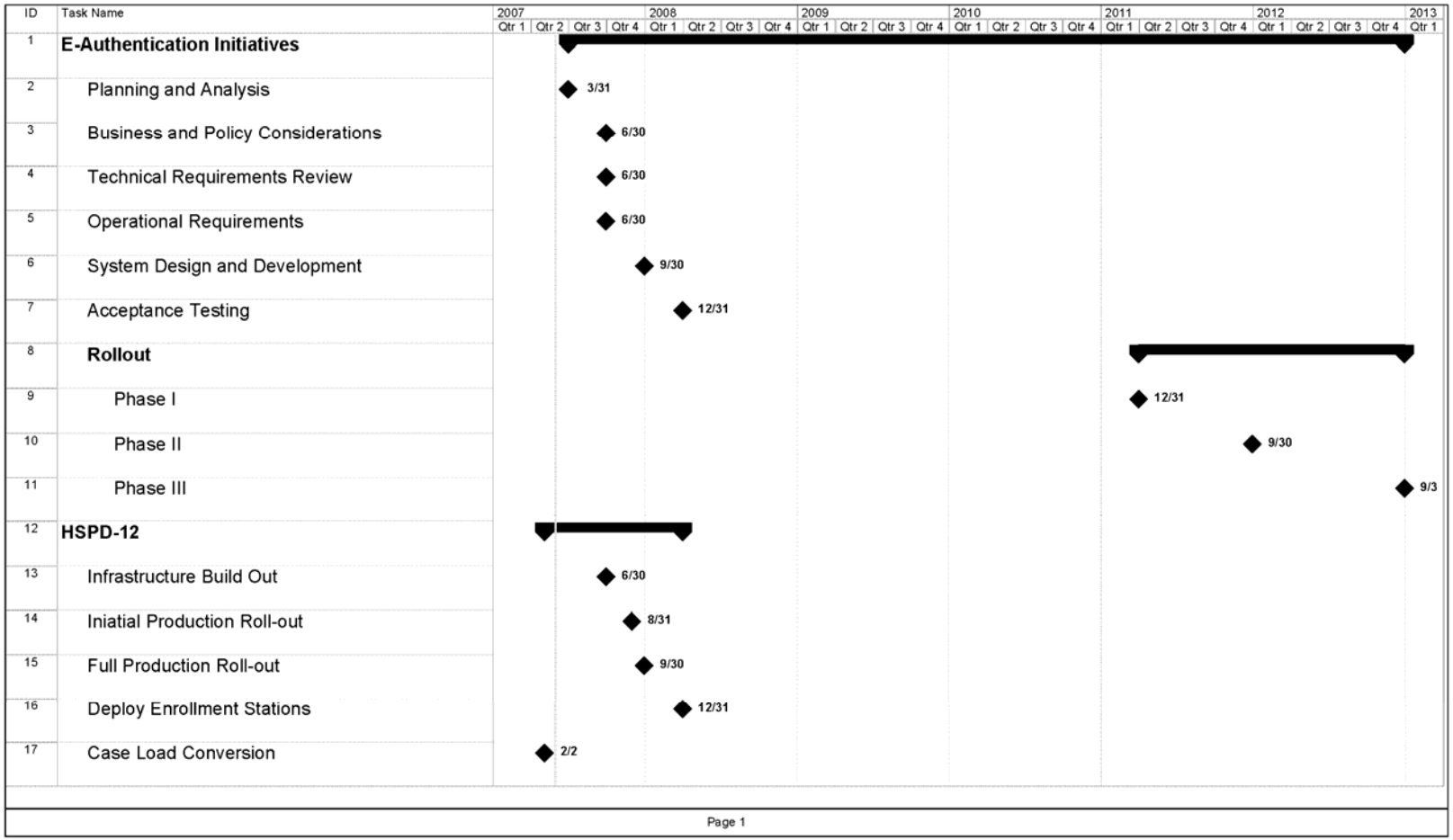
2.17.16 VOIP

For MODERATE- and HIGH-impact systems:

- Establish usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously
- Document, monitor, and control the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.

3 Transition Overview

Figure -- - Transition Overview-



4 Acronyms

C&A - Certification and accreditation
CIO - Chief Information Officer
CNSS - Committee for National Security Systems
DAA - Designated Approving Authority
E.O. - Executive Order
FIPS - Federal Information Processing Standards
FISMA - Federal Information Security Management Act
ISSO - Information systems security officer
IT - Information Technology
NIST - National Institute of Standards and Technology
NIST SP- NIST Special Publication
OCIO - Office of the Chief Information Officer
OMB - Office of Management and Budget
PCSP - Program Cyber Security Plan
P.L. - Public Law
SSP - System Security Plan
ST&E - Security Testing And Evaluation
U.S.C. - United States Code

5 References

1. DOE O 205.1A *Department of Energy Cyber Security Management*
2. DOE CIO Guidance CS-1 *Management, Operational, and Technical Controls Guidance*
3. DOE CIO Guide 205.1-2 *Certification and Accreditation Guide*
4. DOE CIO Guidance CS-3 *Risk Management Guidance*
5. DOE CIO Guidance CS-4 *Vulnerability Management Guidance*
6. DOE CIO Guidance CS-5 *Interconnection Agreements*
7. DOE CIO Guidance CS-6 *Plan of Action and Milestones Guidance*
8. DOE CIO Guidance CS-7 *Contingency Planning Guidance*
9. DOE CIO Guidance CS-12 *Password Management Guidance*
10. DOE CIO Guidance CS-13 *Wireless Devices and Information Systems*
11. DOE CIO Guidance CS-14 *Portable/Mobile Device Guidance*
12. DOE CIO Guidance CS-20 *Information Condition Guidance*
13. DOE CIO Guidance CS-38a *Protection of Sensitive Unclassified Information, Including Personally Identifiable Information*
14. DOE Cyber Security Program *Cyber Security Strategic Plan v.8* January 2007
15. NIST SP800-53 rev1 *Recommended Security controls for Federal Information Systems*
16. NIST SP800-94 (DRAFT) *Guide to Intrusion Detection and Prevention Systems*
17. NIST SP800-83 *Guide to Malware Incident Prevention and Handling*
18. Enterprise Architecture Data Call (December 2006) Malware Protection
19. DOEnet Network & Security Baseline Architecture (DRAFT) April 2006
20. DOE IT Security Segment Architecture Project Scope and Plan April 2006