

# Program Cyber Security Plan

## Cyber Security Requirements for National Security Systems

---

### 1.0 Purpose

The purpose of this document is to provide the Office of Science (SC) a direction on a consistent method to implement cyber security protections for National Security Systems (NSS) in a manner that ensures the security of information and information systems of all Federal and contractor staff while meeting mission requirements, and also to ensure compliance with all Federal laws and Federal and DOE policies and direction regarding the protection of this information. In addition, this MS will aid in the implementation of the federally mandated Certification and Accreditation (C&A) in SC for information systems processing, storing, and/or transmitting National Security information.

### 2.0 Responsibilities

The roles and responsibilities for implementing this document are described in the Office of Science (SC) Program Cyber Security Plan (PCSP) and in the SC NSS PCSP Implementation Manual.

### 3.0 Management System Operation

#### 3.1 Overview

The Office of Science (SC) implements cyber security activities to protect its information and information systems as required by law and by utilizing the principles and recommendations of DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM), National Institute of Standards and Technology (NIST), and the SC NSS PCSP Implementation Manual to secure its National Security systems. SC staff will:

- 1) ensure that applicable implementation guidance is followed by site offices and laboratories;
- 2) ensure that appropriate cyber security implementation guidance is placed into contracts;
- 3) provide oversight of contractor SC sites' policies and guidance cyber security work planning and controls;
- 4) integrate continuous feedback and improvement mechanisms into their work; and
- 5) perform the necessary oversight /assessments of both the Federal staff and contractors.

This MS addresses the requirements for SC staff in protecting National Security (NS) cyber assets and information and the performance of DOE policies and guidance that are

Federal responsibilities. Furthermore, this MS serves to ensure that DOE policies, guidance, and methods of accomplishment are identified, communicated, and implemented by both Federal staff and contractors. This includes the oversight, assessment, and evaluation of both Federal staff and contractor performance, and reporting of cyber security performance data to SC and other entities (e.g., U.S. Department of Energy and, as appropriate, Federal, state, and local governments). Effective implementation of this MS will ensure the security of National Security information and information systems for SC site offices and laboratories.

The processes for addressing contractor NSS PCSP performance expectations are outlined in the respective NSS Cyber Security Program Plans (“Master Plan”) of the SC laboratories and site offices.

## **3.2 Key Functions/Services and Processes**

### **3.2.1 PCSP Subject Areas for Functions/Services and Processes for Federal Staff**

SC PCSP requirements, responsibilities, and authorities for the Federal staff are included in the DOE Order 205.1A, “*Department Of Energy Cyber Security Management.*” The Cyber Security Management (CSM) structure establishes a program whereby the staff plans, performs, assesses, and improves the security of information and information systems within DOE. This program is institutionalized within SC at Headquarters, the Integrated Service Centers, Site Offices and Laboratories, with the development of Cyber Security Program Plans (CSPP) for National Security systems. The following sections describe the SC direction issued by the OCIO to ensure compliance with PCSP requirements. The following subsections correspond to PCSP implementation, to ensure direction is aligned with SC’s mission.

#### **3.2.1.1 Process for Assessing Risk and Securing Cyber Systems**

The Office of Science is committed to ensure that all information systems are protected in accordance with the magnitude of harm that would occur should the information or the information system be compromised or destroyed. Effective and compliant cyber security is the goal of the SC National Security information system cyber security program. This task describes the process by which all the information and information systems are grouped into Protection Levels (PLs) which are protected by various security controls. This task also includes the process by which artifacts are developed or updated; management, operational, and assurance controls are identified; the controls are tested, and an Authority to Operate (ATO) is issued. Section 5.1 contains an overview of this process.

#### **3.2.1.2 Cyber Security Direction for National Security Systems**

The Office of Science is committed to ensuring that the Federal staff performs required Federal program responsibilities in an effective and compliant manner. SC organizations are expected to implement DOE OCIO policy and direction within a security framework

applicable to their mission. SC ensures that Federal and contractor staffs are implementing their PCSP requirements and responsibilities by providing direction on OCIO Cyber Security Technical & Management Requirements (TMRs). This subject area (Section 5.2) identifies the security expectations for compliance with DOE cyber security direction.

### 3.2.1.3 Cyber Security Risk Mitigation Strategies for National Security Systems

SC is committed to providing specific direction on risk analysis to assure that mission requirements are satisfied without compromising the security of the Office of Science or DOE. SC has developed the SC NSS PCSP Implementation Manual to assist sites in determining the consequence of loss (CoL) and protection strategies for NS systems.

## 4.0 Requirements

The following table summarizes high-level requirements relevant to this management system.

| Document Number                 | Title   |
|---------------------------------|---|
| P.L. 103-356                    | Government Management Reform Act of 1994, (October 13, 1994)  |
| P.L. 104-208                    | Title VIII, Federal Financial Management Improvement Act of 1996 (FFMIA), (October 1, 1996).              |
| P.L. 104-231                    | Electronic Freedom of Information Act (e-FOIA), (October 2, 1996)   |
| P.L. 107-347                    | Title III, Federal Information Security Management Act of 2002 (FISMA), (December 17, 2002).              |
| P.L. 93-579                     | Privacy Act of 1974, as amended [Title 5 United States Code (U.S.C.) Section 552a], (December 31, 1974).  |
| P.L. 96-349                     | Trade Secrets Act - (18 U.S.C., section 1905), (January 22, 2002).  |
| P.L. 97-255                     | Federal Managers' Financial Integrity Act of 1982 (FMFIA), (September, 8, 1982)                           |
| P.L. 99-474                     | Computer Fraud and Abuse Act (18 U.S.C. section 1030), (October 16, 1986)                                 |
| P.L. 99-508                     | Electronic Communications Privacy Act of 1986, (October 21, 1986)   |
| P.L. 100-235                    | Computer Security Act of 1987, (January 8, 1988)  |
| P.L. 104-106                    | Division E, Clinger-Cohen Act (Information Technology Management Reform Act of 1996), (February 10, 1996) |
| OMB Circular A-123              | Management Accountability and Control, (August 4, 1986) (revised Dec 21, 2004)                            |
| OMB Circular A-130 Appendix III | Security of Federal Automated Information Resources, (November 2003)                                      |
| OMB Memorandum M-96-20          | Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)               |
| OMB Memorandum M-97-02          | Funding Information Systems Investments, (October 25, 1996)   |

|                            |   |
|----------------------------|---|
| OMB Memorandum<br>M-99-20  | Security of Federal Automated Information Resources, (June 23, 1999)  |
| OMB Memorandum<br>M-00-07  | Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)  |
| OMB Memorandum<br>M-00-10  | OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)  |
| OMB Memorandum<br>M-00-015 | OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)                              |
| OMB Memorandum<br>M-01-08  | Guidance on Implementing the Government Information Security Reform Act, (January 16, 2001)   |
| OMB Memorandum<br>M-01-26  | Component-Level Audits, (July 10, 2001)   |
| OMB Memorandum<br>M-04-25  | FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)             |
| OMB Memorandum<br>M-05-02  | Financial Management Systems, (December 1, 2004)  |
| NIST FIPS 201-1            | National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006) |
| NIST FIPS 200              | Minimum Security Requirements for Federal Information and Information Systems, (March 2006)   |
| NIST FIPS 199              | Standards for Security Categorization of Federal Information and Information Systems, (February 2004)   |
| NIST FIPS 142-2            | Security Requirements for Cryptographic Modules, (May 2001)   |
| NIST 1SP 800-92            | Guide to Computer Security Log Management, (September 2006)   |
| NIST SP 800-88             | Guidelines for Media Sanitization, (September 2006)   |
| NIST SP 800-83             | Guide to Malware Incident Prevention and Handling, (November 2005)  |
| NIST SP 800-70             | The NIST Security Configuration Checklists Program, (May 2005)  |
| NIST SP 800-65             | Integrating Security into the Capital Planning and Investment Control Process, (January 2005)   |
| NIST SP 800-64             | Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)   |
| NIST SP 800-61             | Computer Security Incident Handling Guide, (January 2004)   |

---

1 Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.

|                    |  |
|--------------------|--|
| NIST SP 800-60     | Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004) |
| NIST SP 800-55     | Security Metrics Guide for Information Technology Systems, (July 2003)                             |
| NIST SP 800-53A    | Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)             |
| NIST SP 800-53 R1  | Recommended Security Controls for Federal Information Systems, (December 2006)                     |
| NIST SP 800-50     | Building an Information Technology Security Awareness and Training Program, (October 2003)         |
| NIST SP 800-47     | Security Guide for Interconnecting Information Technology System, (August 2002)                    |
| NIST SP 800-37     | Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)  |
| NIST SP 800-34     | Contingency Planning Guide for Information Technology Systems, (June 2002)                         |
| NIST SP 800-30     | Risk Management Guide for Information Technology Systems, (July 2002)                              |
| NIST SP 800-26, R1 | Guide for Information Security Program Assessments and System Reporting Form, (November 2001)      |
| NIST SP 800-18, R1 | Guide for Developing Security Plans for Federal Information Systems, (February 2006)               |
| DOE O 142.1        | Classified Visits Involving Foreign Nationals, (January 13, 2004)                                  |
| DOE O 142.3        | Unclassified Foreign Visits and Assignments Program, (June 18, 2004)                               |
| DOE P 205.1        | Departmental Cyber Security Management Policy, (May 8, 2001)                                       |
| DOE O 205.1A       | Department of Energy Cyber Security Management Program, (December 4, 2006)                         |
| DOE M 205.1-4      | National Security System (NSS) Manual, (March 8, 2007)   |
| DOE O 221.2        | Cooperation with the Office of Inspector General, (March 22, 2001)                                 |
| DOE P 226.1        | Department of Energy Oversight Policy, (June 10, 2005)   |
| DOE O 226.1        | Implementation of Department of Energy Oversight Policy, (September 15, 2005)                      |
| DOE M 452.4-1A     | Protection of Use Control Vulnerabilities and Design, (March 11, 2004)                             |
| DOE O 457.1        | Nuclear Counterterrorism, (February 7, 2006)   |
| DOE P 470.1        | Integrated Safeguards and Security Management (ISSM) Policy, (May 8, 2001)                         |
| DOE O 470.2B       | Independent Oversight and Performance Assurance Program, (October 31, 2002)                        |
| DOE M 470.4-1      | Safeguards and Security Program Planning and Management, (August 26, 2005)                         |
| DOE M 470.4-2      | Physical Protection, (August 26, 2005)   |
| DOE M 470.4-4      | Information Security, (August 26, 2005)  |
| DOE M 470.4-5      | Personnel Security, (August 26, 2005)  |

|               |  |
|---------------|--|
| DOE O 471.1   | Identification and Protection of Unclassified Controlled Nuclear Information, (June 30, 2000)        |
| DOE O 470.4   | Safeguards and Security Program, (August 26, 2005)   |
| DOE O 475.1   | Counterintelligence Program, (February 10, 2004)   |
| DOE O 5610.2  | Control of Weapon Data, (September 2, 1986)  |
| DoD 5220.22-M | National Industrial Security Program Operating Manual, (February 2006)                               |
| E.O. 12958    | Classified National Security Information, (April 17, 1995)   |
| E.O. 13011    | Federal Information Technology, (July 17, 1996)  |
| HSPD-12       | Policy for a Common Identification Standard for Federal Employees and Contractors, (August 27, 2004) |

## 5.0 Subject Areas

### 5.1 Process for Assessing Risk and Securing Cyber Systems

The Office of Science follows the Federal Information Systems Management Act (FISMA) implementation project model to assess risk and secure information systems. The process is illustrated in Figure 5.1. The approach is comprised of those activities that are specifically required within the FISMA framework and detailed in statutorily required standards and guidance. As illustrated in Figure 5.1 below, these activities are part of a cyclical continuous improvement process, and the conclusion of one cycle starts the next iteration.

Prior to the analysis, system data is collected. This information describes the purpose of the information systems, who owns the systems; what data is collected and the physical location of the servers, and end user devices. Based upon the information collected from existing documentation and interviews with system owners, the Protection Level (PL), and risk impact based on confidentiality, integrity and availability is determined. Each system is categorized based on the highest PL, or level of classification, for the information processed, stored, or transmitted on the system. The baseline controls are then analyzed in light of any decision by Senior DOE Management, SC, the Information Systems Security Manager (ISSM), or the information system owner to increase the CoL (e.g., due to the identification of a threat not identified in the DOE or Site Threat Statement, and/or identification of a standard practice not identified in the control set for a protection level).

Once the overall impact level of the information system is determined, an initial set of security controls are selected from the corresponding control sets based upon the system type (single-user standalone, multi-user, interconnected system, etc.). Sites have the flexibility to tailor the security controls to a more stringent protection level in accordance with the CoL determination. The entirety of this effort is documented in the site NSS CSPP. A set of the National Information Assurance Certification and Accreditation Process (NIACAP) -compliant cyber security documents are then generated which includes a threat statement, risk assessment, CSPP, supplementary controls, etc.

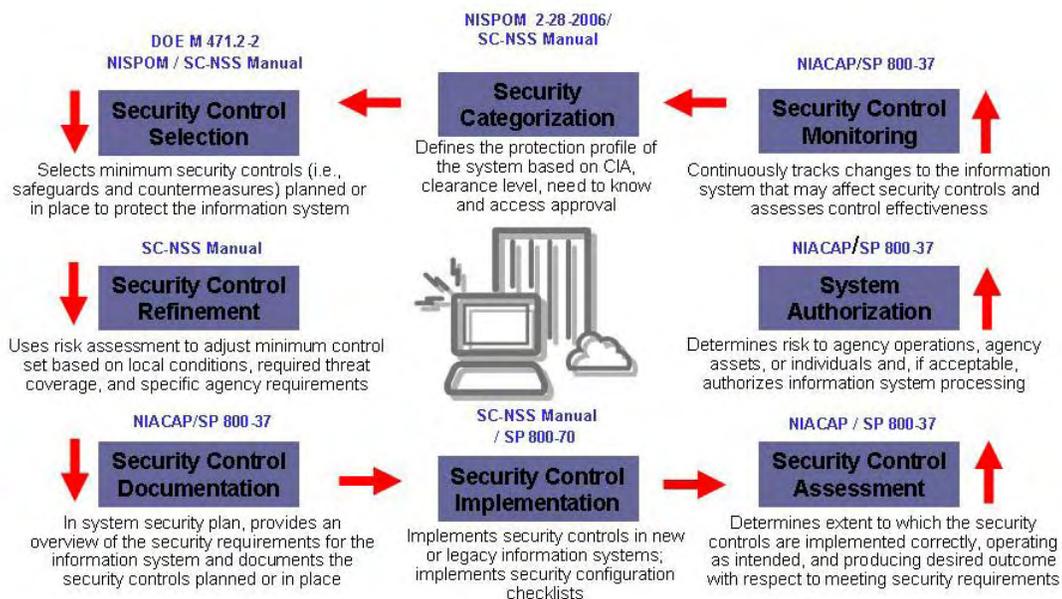


Figure 5.1 FISMA Implementation Project Model

After the controls have been selected and implemented, the controls are tested to ensure that everything functions as specified. This requires the development of an independent Security, Test and Evaluation (ST&E) plan. The results of the ST&E are documented and, along with all the previous documents, are then compiled and provided to the Designation Approving Authority (DAA) to obtain the Authority to Operate.

This last phase provides the DAA with the evidence required to ensure that SC management and staff are made aware of the threats, vulnerabilities and risks; and that the assurance, operational, and technical controls are in place and working. The DAA can then make a rational decision concerning whether or not the system is allowed to operate under these conditions. The DAA is accountable to assure that the agreed upon controls continue to operate as specified throughout the life cycle of the system, or that the operational environment is re-assessed if a significant change to the environment is made.

## 5.2 Cyber Security Direction for National Security Systems

Below is SC's analysis and direction on each of the OCIO Cyber Security (CS) guidance documents<sup>2</sup>. SC complies with statutory requirements, Office of Management and Budget (OMB) requirements, National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) requirements, and Departmental policy. The SC cyber security program is centered on the SC NSS Manual, NIST Special Publication

<sup>2</sup> SC PCSP direction will reflect CIO Cyber Security Guidance until the OCIO Cyber Security Cyber Security Technical and Management Requirements are issued. Updates to OCIO cyber security guidance are shown on <http://cio.energy.gov/policy-guidance/guidance.htm>.

(SP) 800 series and OMB guidance. Each site should review the guidance documents to assure that controls being implemented are consistent with this section. This section will evolve as OCIO CS Guidance is replaced by Technical and Management Requirement (TMR) documents.

The CS numbers correspond to the OCIO's numbering schema and not all numbers are addressed, as some do not apply to National Security systems.

### **CS-01, Management, Operational, and Technical Controls Guidance**

- Analysis -- The document indicates that this is not mandatory for National Security Systems, and that CS-22 will apply. To date, CS-22 is in development.
- SC Direction – SC will implement the SC NSS PCSP Implementation Manual with consideration of the guidance in CS-01. Control implementation and how the site or facility will satisfy that control will be documented in the site NSS Master Plan. The DAA will make the final decision as to the effectiveness of the controls, and when satisfied that the system is operating at an acceptable risk level, will issue an Authority to Operate.

### **CS-02, Certification and Accreditation Guide**

- Analysis -- The document outlines the Certification and Accreditation process. It is generally consistent with the NIST SP 800-37, *“Guide for the Security Certification and Accreditation of Federal Information Systems.”*
- SC Direction – SC will implement the SC NSS PCSP Implementation Manual with consideration of the guidance in CS-02. The DAA will make the final decision as to the effectiveness of the controls, and when satisfied that the system is operating at an acceptable risk level, will issue an Authority to Operate.

### **CS-03, Risk Management Guide**

- Analysis -- The document identifies the process of analyzing cyber security risks and is consistent with NIST SP 800-30, *“Risk Management Guide for Information Technology Systems.”* There is a requirement to use the DOE threat statement as a baseline for the analysis. There is also a requirement to have systems tested and evaluated – SC interprets this to be the Security Test and Evaluation.
- SC Direction – National Security systems are protected at the highest PL for the information stored, processed or transmitted on a system based on compliance with Federal and DOE guidance. Sites may raise the CoL level for a particular control or control set, but may not lower the CoL for NS systems. SC will implement the SC NSS PCSP Implementation Manual with consideration of the guidance in CS-03. Risk is assessed at the site and system level. The threat statements must be

customized to reflect each site's environment, and are currently based on a SC-wide threat statement that reflects the most common vulnerabilities with National Security information systems. The DOE threat statement will also be used when it is issued.

#### **CS-04, Vulnerability Management Guide**

- Analysis -- The document identifies requirements for vulnerability scanning and patching, and is consistent with NIST SP 800-40, "*Creating a Patch and Vulnerability Management Program*" and NIST SP 800-42, "*Guideline on Network Security Testing*". The guidance document states that a risk based approach should be used to determine scanning frequency and that a maximum test period should be established.
- SC Direction -- The SC policy is to implement the SC NSS PCSP Implementation Manual with consideration of the guidance in CS-04. Vulnerability and patch management will be documented in the site NSS CSPP.

#### **CS-05, Interconnection Agreement Guidance**

- Analysis -- The document identifies requirements, processes, and procedures for planning, documenting, and managing system interconnections; and is consistent with NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*". The guidance document requires that the specific hardware and configuration of the connecting systems be identified.
- SC Direction -- The SC policy is to implement the SC NSS PCSP Implementation Manual with consideration of the guidance in CS-05. Interconnection agreements will be documented in the site NSS CSPP.

#### **CS-06, Plan of Actions and Milestones (POA&M) Guidance**

- Analysis -- The document identifies the requirements for developing, documenting, and implementing a Plan of Actions and Milestones (POA&M) process and is consistent with NIST SP 800-37, "*Guide for the Security Certification and Accreditation of Federal Information Systems*." The document requires POA&M items that have been verified and closed to continue to be reported for at least a year. The document also requires the reporting of "no POA&M" items.
- SC Direction -- SC policy is to implement SC NSS PCSP Implementation Manual and consider the guidance in CS-06. However, there will be no POA&M items resulting from the initial on-site portion of a site visit of a SC element for one year. After that period, all items must be reported and tracked through the POA&M process. The site visit leads to enhancement of the cyber security program, implementation of the controls, and upgraded documentation. This results in a

compliant certification and accreditation package for the systems with an accompanying POA&M.

### **CS-07, Contingency Planning Guidance**

- Analysis -- The document identifies contingency planning responsibilities and requirements and is consistent with NIST SP 800-34, “*Contingency Planning Guide for Information Technology Systems*”, and there is general agreement on the purpose and process for establishing a contingency plan. The guidance document requires that contingency plans be developed for Critical Infrastructure or Key Resources (CI/KR), and that contingency plans tests are either functional tests or table-top exercises.
- SC Direction -- SC will implement SC NSS PCSP Implementation Manual with consideration of the supplemental guidance in CS-07. Additionally, SC will implement contingency plans at the Master Plan level. There are some SC facilities which may have limited contingency plans or plans that are less detailed than described in this document. This is typically because the business impact analysis either permits a 5 day restoration period, which can be accomplished with vendor provided equipment, or because backup for the system is not practical. For example, one of a kind experimental or computation facilities, if destroyed, may not be repaired but may be replaced by the next generation of facility or item, or DOE may decide to terminate this capability. SC considers on the job training or replacing key equipment from an information system as a valid substitute for a Contingency Plan test.

### **CS 08, Configuration Management Guidance**

- Analysis -- This guidance document is in concert with best practice for computer security configuration. The requirement is that network devices should support a national minimum security configuration setting. These national setting are determined by Center for Internet Security (CIS), National Security Agency (NSA), or Defense Information Systems Agency (DISA).
- SC Direction -- SC will implement configuration management as described in the SC NSS PCSP Implementation Manual.

### **CS-09, Incident Management Guidance**

- Analysis -- The document contains policy on reporting of cyber security incidents. The guidance contains basically the same text as the DOE Manual 205.1-1, “*Incident Prevention, Warning and Response (IPWAR)*.” The requirements have been enhanced to include loss, theft and missing laptops/IT resources; and improperly purged or sanitized media. There are new reporting requirements for each incident that includes an impact assessment for each incident. Responsibilities for completion of these requirements will be defined in the CSPP or System Security Plan (SSP).

- SC Direction -- SC policy is to implement the SC NSS PCSP Implementation Manual with consideration of the guidance in CS-09. There are new reporting requirements which include an impact assessment for each incident. Responsibilities for completion of these requirements will be defined in the Master Plan. Impact assessments will be sent to the SIO for review and comment.

### **CS-11, Media Clearing, Purging and Destruction Guidance**

- Analysis -- The document provides policy on the cleaning, destruction, and reuse of media. IT has requirements beyond the existing DOE Manual 205.1-2, "*Clearing, Sanitization and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Manual.*" It is prescriptive in the treatment of media reuse and covers substantially more media products than the legacy DOE manual. The policy allows SC to outsource the purging/clearing of media to another DOE facility/agency or authorized contractor. Handling of removable media with National Security information will need to be addressed in the Master Plan.
- SC Direction -- SC policy is to implement the SC NSS PCSP Implementation Manual with consideration of CS-11.

### **CS-12, Password Management Guidance**

- Analysis -- The document provides policy on password structure and guidance to the DOE M 471.3-1, "*Manual for Identifying and Protecting Official Use Only Information.*" There is general agreement on the purpose and process for establishing passwords. The guidance allows for passwords based on entropy which currently cannot be checked for compliance via existing software tools.
- SC Direction -- SC policy is to implement the SC NSS PCSP Implementation Manual with consideration of the guidance in CS-12. SC will only allow passwords that can be checked for rigor with a software tool to test the strength of the password. This means that entropy based passwords are currently excluded. SC supports password change a minimum of every six months or immediately if the password is suspected of compromise.

### **CS-13, Wireless Devices and Information systems Guidance**

- Analysis -- The document provides policy on the use of wireless devices. It is consistent with NIST SP 800-48, "*Wireless Network Security: 802.11, Bluetooth, and Handheld Devices,*" and there is general agreement on the purpose and process for implementation of wireless networks. The document includes prohibitions on downloading freeware/shareware using wireless.

The NIST document on wireless (SP 800-48) is relatively out of date, and some of the concerns with wireless communication have been resolved with newer standards. If

the newer encryption standards are enforced, wireless networking can be used with wired networks. The document also requires an isolated C&A package solely for wireless systems.

- SC Direction – This guidance does not apply to National Security Systems, as wireless is prohibited for use in secure areas.

#### **CS-14, Portable/Mobile Devices Guidance**

- Analysis -- The guidance has been broadened to include personal laptops, PDA/Blackberries, cell phones, MP3 players, and other devices that collect/transmit/store DOE information. The policy requires that portable/mobile devices used to process DOE information, taken outside the United States be, at a minimum, sealed with a tamper indicating device or subject to a hardware/software technical review process upon leaving and re-entering the United States.
- SC Direction -- SC policy is to implement SC NSS PCSP Implementation Manual with consideration for the guidance in CS-14. Specific direction on creating Classified Removable Electronic Media (CREM) is outlined in DOE M 470.4-4, “*Information Security.*”

#### **CS-15, Personally Owned Devices Guidance**

- Analysis -- The guidance states that the PCSP and supporting documentation should have defined policies and procedures for the use of personally owned devices (as opposed to government or contractor provided devices) that are used within the DOE facilities.
- SC Direction – This guidance does not apply to NS systems, as personally-owned devices are prohibited for processing NS information.

#### **CS-18, Foreign National Access to DOE Information Systems Guidance**

- Analysis -- The guidance is consistent with DOE O 142.3, “*Unclassified Foreign Visits and Assignment Program*” in that it recognizes background checks should be dependent on the level of access granted (general user, privileged user and administrator) and type of information being accessed. SC has developed an access policy consistent with this approach.
- SC Direction – CS-15 only covers foreign national access to unclassified systems. For NS systems, SC policy is based on DOE O 142.1, “*Classified Visits Involving Foreign Nationals.*”

## **SC-20, Information Condition (INFOCON) Guidance**

- Analysis -- The document establishes an overall graded approach to cyber security escalation and actions similar to the Department of Homeland Security (five color) levels. The incident reporting process describes actions to be taken in the event of a compromise or suspected compromise, and they are consistent with the guide.

SC Direction -- SC has procedures in place to respond to external threats. Incident procedures, as well as the normal controls in place for information security result in a posture consistent with “code yellow.” Each site has the capability to shut off specific ports, applications, or processes in the event of a suspected attack, or to facilitate forensic analysis. The INFOCON process is part of overall incident reporting/alert procedures and is managed centrally by the DOE’s Chief Information Officer. SC policy is to take CS-20 under consideration.

## **CS-23, Peer to Peer Networking (P2P) Guidance**

- Analysis -- The document is concerned with the legal and ethical security aspects of P2P networking.
- SC Direction – CS-23 is not applicable, as P2P networking is prohibited on NS systems.

## **CS-24, Remote Access Guidance**

- Analysis -- This guidance identifies measures related to accessing DOE and contractor information systems from outside of the enclave or accreditation boundary. Implementation of the controls in NIST 800-53, “*Recommended Security Controls for Federal Information Systems*,” with consideration of the guidance in CS-24, is an access control issue.
- SC Direction -- SC policy on remote access is governed through the interconnection agreement as discussed in the SC NSS PCSP Implementation Manual. Consideration will be given to the guidance in CS-24.

## **CS-37, Security Testing Guidance**

- Analysis -- This guidance for implementing a Security, Test and Evaluation (ST&E) as part of the C&A process for National Security systems aligns with NIST SP 800-37.
- SC Direction -- SC policy is to implement NIST SP 800-37 with consideration of the guidance in CS-37.

## CS-38A, Protection of Sensitive Unclassified Information including Personally Identifiable Information Guidance

- Analysis -- This document aligns with new the OMB direction for handling Personally Identifiable Information (PII). All mobile/portable devices are assumed to contain PII or Sensitive Unclassified Information (SUI) and must be protected in accordance with a NIST FIPS 140-2 compliant encryption. Exceptions to this policy are to be documented in the PCSP.
- SC Direction – PII is not considered NS information, and therefore this CS does not apply.

### 6.0 References

The following table summarizes high-level references relevant to this management system.

| Document Number                 | Title   |
|---------------------------------|---|
| P.L. 103-356                    | Government Management Reform Act of 1994, (October 13, 1994)  |
| P.L. 104-208                    | Title VIII, Federal Financial Management Improvement Act of 1996 (FFMIA), (October 1, 1996).              |
| P.L. 104-231                    | Electronic Freedom of Information Act (e-FOIA), (October 2, 1996)   |
| P.L. 107-347                    | Title III, Federal Information Security Management Act of 2002 (FISMA), (December 17, 2002).              |
| P.L. 93-579                     | Privacy Act of 1974, as amended [Title 5 United States Code (U.S.C.) Section 552a], (December 31, 1974).  |
| P.L. 96-349                     | Trade Secrets Act - (18 U.S.C., section 1905), (January 22, 2002).  |
| P.L. 97-255                     | Federal Managers' Financial Integrity Act of 1982 (FMFIA), (September, 8, 1982)                           |
| P.L. 99-474                     | Computer Fraud and Abuse Act (18 U.S.C. section 1030), (October 16, 1986)                                 |
| P.L. 99-508                     | Electronic Communications Privacy Act of 1986, (October 21, 1986)   |
| P.L. 100-235                    | Computer security Act of 1987, (January 8, 1988)  |
| P.L. 104-106                    | Division E, Clinger-Cohen Act (Information Technology Management Reform Act of 1996), (February 10, 1996) |
| OMB Circular A-123              | Management Accountability and Control, (August 4, 1986) (revised Dec 21, 2004)                            |
| OMB Circular A-130 Appendix III | Security of Federal Automated Information Resources, (November 2003)                                      |
| OMB Memorandum M-96-20          | Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)               |
| OMB Memorandum M-97-02          | Funding Information Systems Investments, (October 25, 1996)   |
| OMB Memorandum                  | Security of Federal Automated Information Resources, (June  |

|                            |   |
|----------------------------|---|
| M-99-20                    | 23, 1999)   |
| OMB Memorandum<br>M-00-07  | Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)  |
| OMB Memorandum<br>M-00-10  | OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)  |
| OMB Memorandum<br>M-00-015 | OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)                              |
| OMB Memorandum<br>M-01-08  | Guidance on Implementing the Government Information Security Reform Act, (January 16, 2001)   |
| OMB Memorandum<br>M-01-26  | Component-Level Audits, (July 10, 2001)   |
| OMB Memorandum<br>M-04-25  | FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)             |
| OMB Memorandum<br>M-05-02  | Financial Management Systems, (December 1, 2004)  |
| NIST FIPS 201-1            | National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006) |
| NIST FIPS 200              | Minimum Security Requirements for Federal Information and Information Systems, (March 2006)   |
| NIST FIPS 199              | Standards for Security Categorization of Federal Information and Information Systems, (February 2004)   |
| NIST FIPS 142-2            | Security requirements for Cryptographic Modules, (May 2001)   |
| NIST 3SP 800-92            | Guide to Computer Security Log Management, (September 2006)   |
| NIST SP 800-88             | Guidelines for Media Sanitization, (September 2006)   |
| NIST SP 800-83             | Guide to Malware Incident Prevention and Handling, (November 2005)  |
| NIST SP 800-70             | The NIST Security Configuration Checklists Program, (May 2005)  |
| NIST SP 800-65             | Integrating Security into the Capital Planning and Investment Control Process, (January 2005)   |
| NIST SP 800-64             | Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)   |
| NIST SP 800-61             | Computer Security Incident Handling Guide, (January 2004)   |
| NIST SP 800-60             | Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)  |

---

3 Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.

|                  |   |
|------------------|---|
| NIST SP 800-55   | Security Metrics Guide for Information Technology Systems, (July 2003)                            |
| NIST SP 800-53A  | Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)            |
| NIST SP 800-53R1 | Recommended Security Controls for Federal Information Systems, (December 2006)                    |
| NIST SP 800-50   | Building an Information Technology Security Awareness and Training Program, (October 2003)        |
| NIST SP 800-47   | Security Guide for Interconnecting Information Technology Systems, (August 2002)                  |
| NIST SP 800-37   | Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004) |
| NIST SP 800-34   | Contingency Planning Guide for Information Technology Systems, (June 2002)                        |
| NIST SP 800-30   | Risk Management Guide for Information Technology Systems, (July 2002)                             |
| NIST SP 800-26R1 | Guide for Information Security Program Assessments and System Reporting Form, (November 2001)     |
| NIST SP 800-18R1 | Guide for Developing Security Plans for Federal Information Systems, (February 2006)              |
| DOE O 142.1      | Classified Visits Involving Foreign Nationals,(January 13, 2004)                                  |
| DOE O 142.3      | Unclassified Foreign Visits and Assignments Program, (June 18, 2004)                              |
| DOE P 205.1      | Departmental Cyber Security Management Policy, (May 8, 2001)                                      |
| DOE O 205.1A     | Department of Energy Cyber Security Management Program, (December 4, 2006)                        |
| DOE M 205.1-4    | National Security System (NSS) Manual, (March 8, 2007)  |
| DOE O 221.2      | Cooperation with the Office of Inspector General, (March 22, 2001)                                |
| DOE P 226.1      | Department of Energy Oversight Policy, (June 10, 2005)  |
| DOE O 226.1      | Implementation of Department of Energy Oversight Policy, (September 15, 2005)                     |
| DOE M 452.4-1A   | Protection of Use Control Vulnerabilities and Design, (March 11, 2004)                            |
| DOE O 457.1      | Nuclear Counterterrorism, (February 7, 2006)  |
| DOE P 470.1      | Integrated Safeguards and Security Management (ISSM) Policy, (May 8, 2001)                        |
| DOE O 470.2B     | Independent Oversight and Performance Assurance Program, (October 31, 2002)                       |
| DOE M 470.4-1    | Safeguards and Security Program Planning and Management, (August 26, 2005)                        |
| DOE M 470.4-2    | Physical Protection, (August 26, 2005)  |
| DOE M 470.4-4    | Information Security, (August 26, 2005)   |
| DOE M 470.4-5    | Personnel Security, (August 26, 2005)   |
| DOE O 471.1      | Identification and Protection of Unclassified Controlled Nuclear Information, (June 30, 2000)     |

|               |  |
|---------------|--|
| DOE O 470.4   | Safeguards and Security Program, (August 26, 2005)   |
| DOE O 475.1   | Counterintelligence Program, (February 10, 2004)   |
| DOE O 5610.2  | Control of Weapon Data (September 2, 1986)   |
| DoD 5220.22-M | National Industrial Security Program Operating Manual (February 2006)  |
| E.O. 12958    | Classified National Security Information, (April 17, 1995)   |
| E.O. 13011,   | Federal Information Technology, (July 17, 1996)  |
| HSPD-12       | Policy for a Common Identification Standard for Federal Employees and Contractors, (August 27, 2004)             |
| CS-01         | Management, Operational and Technical Controls Guidance, (July 6, 2006)  |
| CS-02         | Certification and Accreditation, (March 24, 2006)  |
| CS-03         | Risk Management, (June 30, 2006)   |
| CS-04         | Vulnerability Management, (July 31, 2006)  |
| CS-05         | Interconnect Agreements, (July 31, 2006)   |
| CS-06         | Plans of Actions and Milestones (POA&M), (September 7, 2006)   |
| CS-07         | Contingency Planning, (August 26, 2006)  |
| CS-08         | Configuration Management, (November 27, 2006)  |
| CS-09         | Incident Management, (January 2007)  |
| CS-11         | Clearing and Media Sanitization (January 2007)   |
| CS-12         | Password Management, (June 30, 2006)   |
| CS-13         | Wireless Devices and Information Systems, (June 30, 2006)  |
| CS-14         | Portable/Mobile Devices, (January 2007)  |
| CS-15         | Personally Owned Devices, (January 2007)   |
| CS-18         | Foreign National Access to DOE Information Systems, (January 2007)   |
| CS-20         | INFOCON, (December 6, 2006)  |
| CS-23         | Peer-To Peer Networking, (December 2006)   |
| CS-24         | Remote Access, (January 2007)  |
| CS-37         | Security, Testing and Evaluation, (January 2007)   |
| CS-38A        | Protection of Sensitive Unclassified Information, including Personally Identifiable Information, (November 2006) |