Policy Letter: NAP-14.2-B

Date: September 27, 2006

TITLE: Baseline Cyber Security Requirements

Table of Contents

1. OBJECTIVES.

   a. Establish requirements and responsibilities for cyber security incident preparation, prevention, warnings, reporting, and recovering from cyber security incidents involving National Nuclear Security Administration (NNSA) information systems.

b. Establish requirements for the use of personally owned or Government owned Personal Electronic Devices (PEDs) and portable computers, hereafter-called portable computing devices, in the NNSA and all organizations under its cognizance.

c. Establish requirements for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified NNSA information systems, applications, and resources.

d. Establish requirements and guidance for standardized procedures and responsibilities for authorizing and communicating Information Conditions (INFOCONs) throughout the NNSA.

e. Establish minimum security controls that are to be enforced by NNSA sites using wireless technologies

f. Establish minimum requirements for remote access to NNSA information systems, applications, and resources.

2. CANCELLATIONS/IMPLEMENTATIONS.

a. NAP.14.2A, BASELINE CYBER SECURITY REQUIREMENTS, 4-05-06. Cancellation of a Policy or Manual does not, by itself, modify, or otherwise affect any contractual obligation to comply with the Policy or Manual. Cancelled Policies and Manuals that are incorporated by reference in a contract remain in effect until the contract is modified to delete the references to the requirements in the cancelled Policy or Manual.

b. This NAP implements DOE M 205.1-1, *Incident Prevention, Warning, and Response (IPWAR) Manual,* DOE N 205.3, *Password Generation, Protection, and Use*, DOE N 205.8, *Cyber Security Requirements for Wireless Devices and Information Systems,* DOE N 205.11, *Security Requirements for Remote Access to DOE and Applicable Contractor Information Technology Systems*, and DOE CIO Guidance CS 38, *Protection of Personally Identifiable Information.*

3. APPLICABILITY. This NNSA Policy (NAP) applies to all entities, Federal or contractor, that collect, create, process, transmit, store, and disseminate information for the NNSA.

a. NNSA Sites. NNSA Headquarters Organizations, Service Center, Site Offices, NNSA contractors, and subcontractors are, hereafter, referred to as NNSA sites.

b. Information System. This NAP applies to any information system that collects, creates, processes, transmits, stores, and disseminates unclassified or classified NNSA information. This NAP applies to any information system lifecycle, including the development of new information systems, the incorporation of information systems into an infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and

legacy systems. In this document, the term(s) "information system," “cyber system,” “Target of Evaluation” (TOE), or "system" are used to mean any information system or network that is used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of NNSA or DOE.

c. Deviations. Deviations from the requirements prescribed in this NAP must be processed in accordance with the requirements in Attachment 1, Chapter E, NAP 14.1-B, *NNSA Cyber Security Program*.

d. Site/Facility Management Contractors. Except for the exclusions in paragraphs 3.e, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this NNSA Policy (NAP) that will apply to site/facility management contractors whose contracts include the CRD.

(1) The CRD must be included in site/facility management contracts that provide automated access to NNSA information or information systems.

(2) The CRD does not automatically apply to other than site/facility management contractors. Any application of requirements of this Policy to other than site/facility management contractors will be communicated separately.

(3) As the laws, regulations, and DOE and NNSA Directives clause of site/facility management contracts states, regardless of the performer of the work, site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD.

(a) Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure the site/facility management contractors’ compliance with the requirements.

(b) Contractors must not flow down requirements to subcontractors unnecessarily or imprudently. That is, contractors will—

i. Ensure that they and their subcontractors comply with the requirements of the CRD; and

ii. Incur only costs that would be incurred by a prudent person in the conduct of competitive business

e. Exclusion. The Deputy Administrator for Naval Reactors shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (set forth in Public Law 106-65 of October 5, 1999 [50 U.S.C. 2406]) and to ensure consistency throughout the joint Navy and DOE Organization of the Naval Reactors Propulsion Program, implement and

oversee all requirements and practices pertaining to this policy for activities under the Deputy Administrator's cognizance.

f. Implementation. A plan for the implementation of this NAP must be completed within 60 days after issuance of this NAP.

NOTE: This NAP does not address contamination of unclassified information systems with classified information (See DOE M 470.4-1 Safeguards and Security Program Planning and Management.

4. RESPONSIBILITIES. Roles and responsibilities for all activities in the NNSA PCSP are described in NAP 14.1-B *NNSA Cyber Security Program*.

5. REQUIREMENTS.

a. Implement the criteria and processes for cyber security incident prevention, warning, and response involving NNSA information systems as described in Attachment 1, Chapter A.

b. Implement the criteria and processes for the use of personally owned or Government-owned Personal Electronic Devices (PEDs) and portable computers, hereafter called portable computing devices, as described in Attachment 1, Chapter B.

c. Implement the generation, protection, and use of passwords to support authentication when accessing classified and unclassified NNSA information systems, applications, and resources as described in Attachment 1, Chapter C.

d. Develop and implement standardized procedures for authorizing and communicating Information Conditions (INFOCONs) throughout the NNSA as described in Attachment 1, Chapter D.

e. Implement the use of wireless technology with NNSA information systems that operationally require such technology as described in Attachment 1, Chapter E.

f. Implement remote access to NNSA information systems that operationally require remote access as described in Attachment 1, Chapter F.

6. CONTACT. Questions concerning this NAP should be directed, through the cognizant Cyber Security Office Manager, to the NNSA Cyber Security Program Manager at 301-903-2425.

7. DEFINITIONS. See Attachment 2.

Linton Brooks
Administrator

Attachments

ATTACHMENT 1

CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) establishes the requirements for National Nuclear Security Administration contractors, with access to NNSA and DOE information systems (Targets of Evaluation). Contractors must comply with the requirements listed in the CRD.

The contractor will ensure that it and its subcontractors cost-effectively comply with the requirements of this CRD.

Regardless of the performer of the work, the contractor is responsible for complying with and flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor must not unnecessarily or imprudently flow down requirements to subcontractors. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

REQUIREMENTS.

1. The contractor shall implement the criteria and processes for cyber security incident preparation, prevention, warning, reporting, and recovery involving NNSA information systems as defined in Chapter A.

2. The contractor shall implement the criteria and processes for the use of personally owned or Government-owned Personal Electronic Devices (PEDs) and portable computers, hereafter called portable computing devices, are defined in Chapter B.

3. The contractor shall implement the generation, protection, and use of passwords to support authentication when accessing classified and unclassified NNSA information systems, applications, and resources as described in Chapter C.

4. The contractor shall develop and implement standardized procedures and responsibilities for authorizing and communicating Information Conditions (INFOCONs) throughout the NNSA as described in Chapter D.

5. The contractor shall implement the use of wireless technology as described in Chapter E.

6. The contractor shall implement remote access to NNSA information systems operationally requiring remote access as described in Chapter F.

This page intentionally blank.

CHAPTER A

REPORTING AND RESPONDING TO CYBER SECURITY INCIDENTS AND ALERTS

1. INTRODUCTION. This chapter establishes the minimum criteria and processes for reporting and responding to cyber security incidents involving NNSA information systems.

2. REPORTING CRITERIA AND PROCESSES.

   a. Reportable Cyber Security Incidents. The site's Cyber Security Program Plan (CSPP) must document the processes for reporting cyber security incidents. Cyber security related incidents must be reported that meet one or more of the following criteria:

      (4) Incidents of Security Concern. Report the cyber security aspects of the following Incidents of Security Concern involving National Security Systems, as adapted from DOE M 470.4.1, Attachment 2, Part 2, Section N *, Safeguards and Security Program Planning and Management.*

      (5) Impact Measurement Index (IMI-1). Reports incidents that pose an immediate danger or short-term threat to National security interests and/or critical NNSA or Department of Energy (DOE) assets, potentially create a serious security situation, or create high media visibility interest. The following cyber security incidents must be reported according to the procedures in this NAP, *in addition to the reporting requirements in DOE M 470.4-1*. These incidents must be reported within 1 working hour of discovery.

         - Confirmed or suspected loss, theft, diversion, or unauthorized release of Weapon Data contained in an information system or on cyber media.
         - Confirmed or suspected loss, theft, diversion, unauthorized release of TOP SECRET information or Special Access Program (SAP) information contained in an information system or on cyber media.
         - Confirmed or suspected intrusions, hacking, or break-ins into NNSA information systems containing TOP SECRET or SAP information.

      (c) Impact Measurement Index (IMI-2). Reports incidents that pose a near- or long-term threat to national security interests and/or critical NNSA or DOE assets, or potentially create a crisis or dangerous situation. The following cyber security incidents must be reported according to the procedures in this NAP, *in addition to any other reporting.* These incidents must be reported within 8 working hours of discovery.

- Confirmed or suspected intrusions, hacking, or break-ins into NNSA information systems or cyber media, containing Confidential Non-Nuclear Weapons Information or Secret Restricted Data Information (as defined in Attachment 1, Chapter G, NAP 14.1-B, *NNSA Cyber Security Program*).
- Loss of classified information that must be reported to other Government agencies or foreign associates.
- The loss of any DOE classified information involving NNSA information systems or cyber media, which requires state or local government or other Federal agency notification.

(d) Impact Measurement Index (IMI-3). Report incidents that pose long-term threats to NNSA or DOE security interests or that potentially degrade the overall effectiveness of the NNSA or the Department's protection programs. The following cyber security incidents must be reported according to the procedures in this NAP, *in addition to any other reporting.* These incidents must be reported within 8 working hours of discovery.

- Confirmed or suspected unauthorized disclosure, loss/potential loss of CONFIDENTIAL matter via intrusions, hacking, or break-ins into NNSA information systems or cyber media.
- Confirmed or suspected unauthorized disclosure, loss/potential loss of Unclassified Mandatory Protection Information (as defined in Attachment 1, Chapter G, NAP 14.1-B, *NNSA Cyber Security Program*) via intrusions, hacking, or break-ins into NNSA information systems or loss/potential loss of cyber media.

(6) Incidents of NNSA Cyber Security Concern. These incidents must be reported based on the Type and System Impact Category. Incidents may be, but not limited to, the result of cyber security alerts received and investigated by the Site.

(a) Type 1 incidents are successful incidents that potentially create serious breaches of DOE/NNSA cyber security or have the potential to generate negative media interest. The following are the currently defined Type 1 incidents.

i. *Compromise/Intrusion*. All unintentional or intentional instances of system compromise or intrusion by unauthorized persons must be reported, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.

ii. *Web Site Defacement*. All instances of a defaced Web site must be reported.

iii. *Malicious Code*. All instances of successful or large network or site-wide infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms, must be reported.

iv. *Denial of Service*. Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or one or more large portions of a network must be reported.

v. *Critical Infrastructure Protection (CIP)*. Any activity that adversely affects an asset identified as critical infrastructure must be reported. NNSA CIP assets are determined by the NNSA Administrator.

vi. *Unauthorized Use*. Unauthorized use should be construed as any activity that adversely affects an information system's normal, baseline performance and/or is not recognized as being related to NNSA's mission. For example, unauthorized use can be using a DOE/NNSA computer to obtain Government data without authorization. Unauthorized use can involve using systems to break the law. Unauthorized use includes, but is not limited to, port scanning that excessively degrades performance; IP (Internet protocol) spoofing; network reconnaissance; monitoring; hacking into servers; running traffic-generating applications that generate unnecessary network broadcast storms or drive large amounts of traffic to computers; or using illegal (or misusing copyrighted) software images, applications, data, and music.

(b) Type 2 incidents are attempted incidents that pose potential long-term threats to DOE/NNSA cyber security interests or that may degrade the overall effectiveness of the Department's cyber security posture. The following are the currently defined Type 2 incidents.

i. *Attempted Intrusion*. A significant and/or persistent attempted intrusion is an exploit that stands out above the daily activity or noise level, as determined by the system owner, and would result in unauthorized access (compromise) if the system were not protected.

ii. *Reconnaissance Activity*. Persistent surveillance and resource mapping probes and scans are those that stand out above the daily activity or noise level and represent activity that is designed to collect information about vulnerabilities in a network and to map network resources and available services.

(c) System Impact Categories. System impact categories characterize the potential impact of incidents that compromise DOE/NNSA information and information systems. Such incidents may impact DOE/NNSA operations, assets, individuals, mission, or reputation. System impact categories identify the level of sensitivity and criticality of information

and information systems by assessing the impact of the loss of confidentiality, integrity, and availability. Performing this impact analysis is a fundamental step in risk assessment. Each of the security objectives—confidentiality, integrity, and availability—is assessed in the following manner.

i. Low Impact. Loss of system confidentiality, integrity, and availability could be expected to have a limited adverse effect on DOE/NNSA operations, assets, or individuals, requiring minor corrective actions or repairs.

ii. Moderate Impact. Loss of system confidentiality, integrity, and availability could be expected to have a serious adverse effect on DOE/NNSA operations, assets, or individuals, including significant degradation or major damage, requiring extensive corrective actions or repairs.

iii. High impact. Loss of system confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on DOE/NNSA operations, assets, or individuals. The incident could cause the loss of mission capability for a period that poses a threat to human life or results in the loss of major assets.

Table 1. Required Time Frame for Reporting Cyber Security Incidents to the Incident Assurance Response Center (IARC)

	System Impact Category		
Incident Type	**Low**	**Moderate**	**High**
Type 1	Within 4 hours	Within 1 hour	Within 1 hour
Type 2	Within 1 week	Within 24 hours	Within 24 hours
Personally Identifiable Information (PII)*	Within 35 minutes	Within 35 minutes	Within 35 minutes

* Based on mandated reporting requirements for PII, all suspected or confirmed incidents involving PII must be reported within 35 minutes regardless of the Type or System Impact. See definition and examples in Attachment 2 for further clarification.

b. Cyber Security Incident Reporting Protocol. Figure 1 illustrates the process for reporting NNSA cyber security incidents. For PII, see figures 2 and 3.

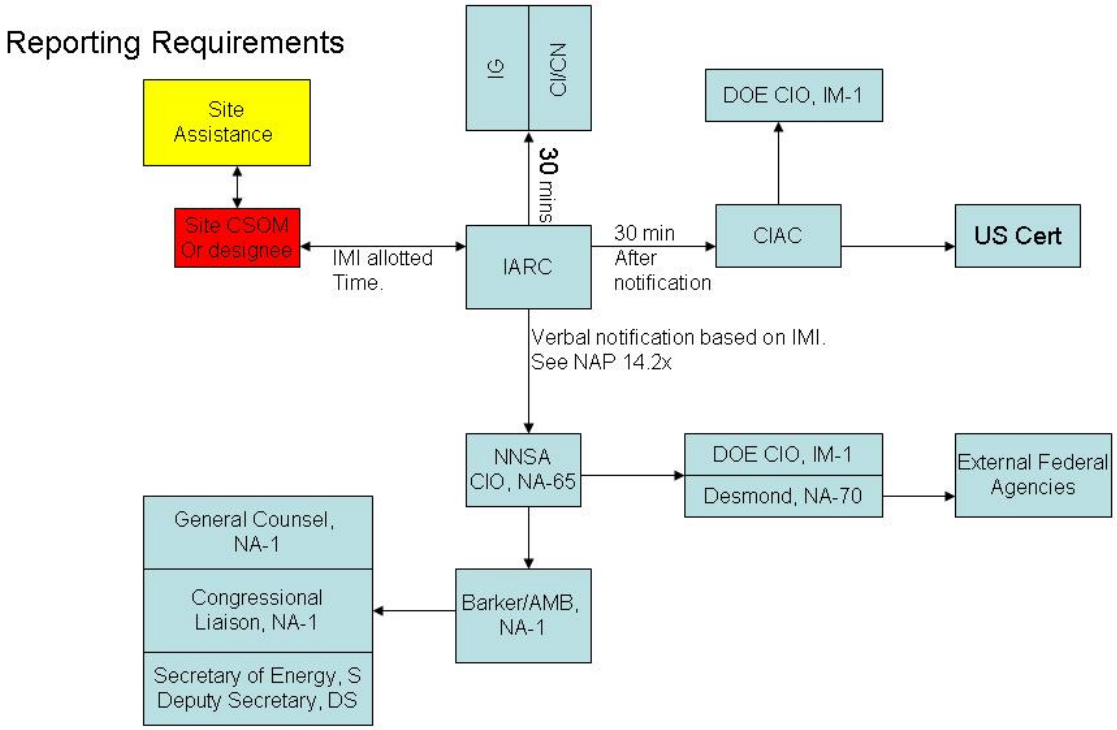

Figure 1. NNSA Cyber Security Incident Reporting Process

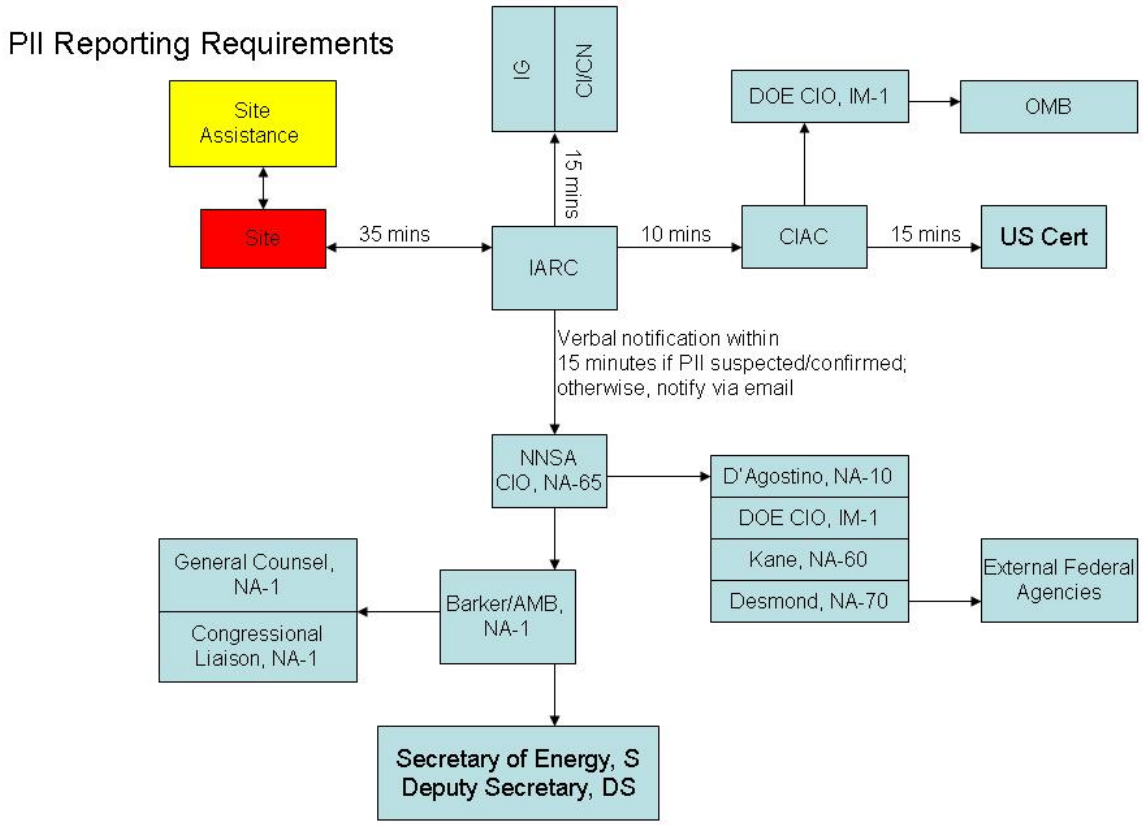

Figure 2. NNSA PII Cyber Security Incident Reporting Process

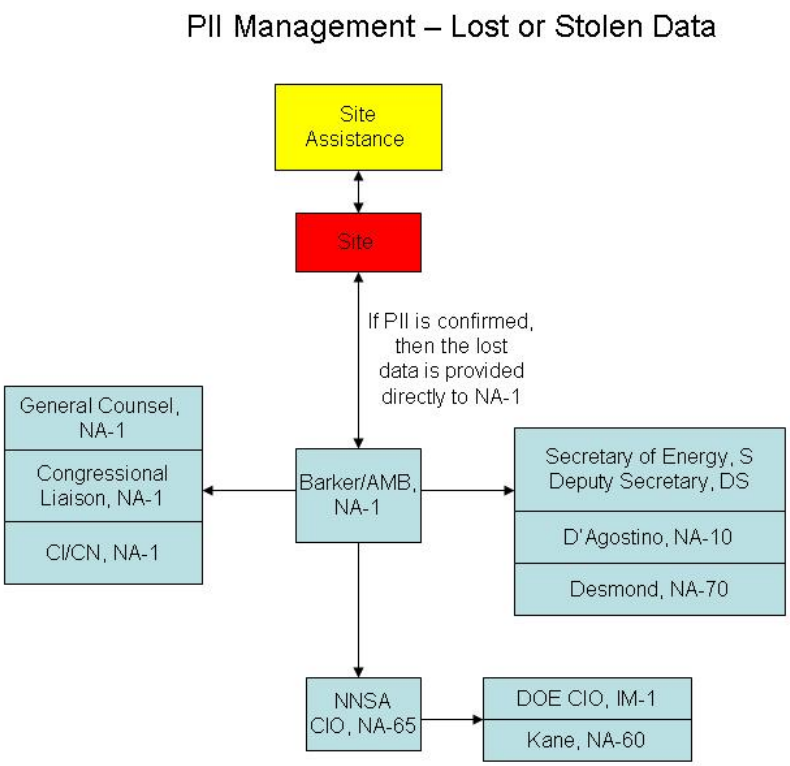

Figure 3. NNSA PII Management – Lost or Stolen Data Process Flow

(1) The cognizant Cyber Security Office Manager (CSOM) must be notified, within 24 hours of discovery of an incident by the NNSA site.

(2) Cyber Security Incident Report Content. The content and format of an incident report will be specified by the cognizant CSOM. At a minimum, incident reports (as defined in paragraph 2) will include date(s), time(s), type, source, corrective actions taken (if any), resources affected, site impact, and site point-of-contact. Source may vary depending on the type of attack, but include Internet Protocol (IP) address, electronic mail (email) address, or other identifying characteristics of the source.

(3) Incidents Involving PII. All suspected or confirmed cyber security incidents involving PII as defined in Attachment 2, *Definitions*, must be reported to the Information Assurance and Response Center (IARC) within 35 minutes of discovery. This notification can be verbal or written via e-mail. As additional information is discovered pertaining to the incident, the impacted site must provide IARC with the updated information within 35 minutes. If an impacted site (i.e., primary) has

solicited the assistance of another site (i.e., secondary) during the investigation, the primary site has the responsibility for reporting all information to IARC.

(4) Archiving Cyber Security Incident Information. Sites must store all information related to a reportable incident, as defined in section 2.a, for at least one year. Storage methods, including custody, must comply with applicable evidentiary requirements for possible future law enforcement use.

(5) Counterintelligence Reporting. Events identified in DOE O 475.1, *Counterintelligence Program*, must be reported by the cognizant CSOM to the Office of Counterintelligence in accordance with the reporting procedures in DOE O 475.1.

(6) Automated Systems. Automated systems may be used to implement these protocols.

c. CIAC Cyber Security Alerts. Cyber security alerts issued by CIAC shall be investigated, analyzed, and reported as an incident. Positive feedback from the sites is required in response to an alert, and the incident reporting mechanism provides the necessary information.

CHAPTER B

PERSONAL ELECTRONIC DEVICES AND PORTABLE COMPUTERS

1. INTRODUCTION. This Chapter establishes the minimum security criteria and processes for the use of personally owned or Government-owned Personal Electronic Devices (PEDs) and portable computers, hereafter called portable computing devices, in the National Nuclear Security Administration (NNSA) and all organizations under its cognizance. This chapter applies to any portable computing device (see definition in Attachment 2) that collects, stores, transmits, or processes unclassified or classified NNSA information or is located in any security area (Property Protection Area (PPA), Limited Area (LA), Exclusion Area (EA), or Protected Area (PA)) where NNSA information systems are used.

2. CRITERIA AND PROCESSES.

   a. Visitors to any NNSA Property Protection, Limited, Exclusion, or Protected Area must be advised, prior to entry, of these criteria and processes.

   b. Non-Government-owned portable computing devices:

      (1) Are prohibited from use within any NNSA Limited, Exclusion, or Protected Area;

      (2) May be used within an NNSA Property Protection Area only in accordance with the procedures defined in the NNSA site's Cyber Security Program Plan (CSPP);

      (3) Are prohibited from any connection (i.e., assigned a network address) to any NNSA or NNSA-contractor local area network, wide area network, or information system component, except as described in the NNSA site's CSPP; are prohibited from storing, processing, receiving, or transmitting classified information; and

      (4) May be used to store, process, receive, or transmit unclassified information with a confidentiality Consequence of Loss of "Medium" or less only in accordance with the policies and procedures defined in the NNSA site's CSPP.

   c. US Government-owned portable computing devices with radio frequency (RF) or Infra-red (IR) capability (e.g. Wireless Information System (W-IS)) may be used in NNSA Property Protection, Limited, Exclusion, and Protected Areas where sensitive unclassified or classified information is processed, stored, transferred, or accessed on information systems, or where sensitive unclassified or classified information is discussed or displayed via electronic methods after completion of a risk assessment of the specific intended use and only if the portable computing device:

(1) Authenticates all users in accordance with the process described in an approved System Security Plan;

(2) Employs up-to-date malicious code detection software;

(3) Applies National Security Agency (NSA)-approved type 1 encryption on all communications to and from the portable computing device involving classified information;

(4) Complies with applicable National Telecommunications and Information Administration (NTIA) and Federal Communication Commission (FCC) requirements;

(5) Complies with NNSA PCSP requirements;

(6) Configured with preferences and settings for services approved by the cognizant DAA;

(7) Configuration managed and controlled; and

(8) Applies DOE approved encryption algorithms on all communications involving sensitive unclassified information.

(9) Encrypt all data on the mobile computer/device which carries agency data unless the data is determined to be non-sensitive, and formally documented, by the NNSA Administrator or their designate.

d. All portable computing devices with an audio recording capability are used in NNSA Property Protection, Limited, Exclusion, or Protected Areas in accordance with NNSA TEMPEST and TSCM policies and the NNSA site's CSPP.

e. The administrative and physical controls, including TEMPEST, and the minimum security configurations used to reduce the risks from the use of any portable computing devices must be documented in the site's CSPP.

f. Site personnel must be trained on the rules of use for portable computing devices that are allowed on NNSA sites. This training must be documented.

g. Supervisory personnel for an individual (Federal or contractor) must be notified of any violation of NNSA policies or site portable computing device procedures. The responsible supervisory personnel must take disciplinary action in accordance with the NNSA site's personnel performance evaluation system.

h. Portable computing devices used at a location, outside the United States, other than the assigned user's primary work location ("home" site of the user) must be sealed with NNSA-approved tamper-indicating devices prior to removal of the portable computing device from the "home" site. The tamper-indicating devices must be placed to allow normal use (i.e., removal and insertion of components such as removable hard drives and batteries). The

hardware and software technical review process for all portable computing devices must be documented in the site's CSPP. The cognizant DAA may approve alternative protection measures when the use of tamper-indicating devices are ineffective or because of operational requirements.

i. If portable computing devices are operated as desktop units (i.e., they do not leave the user's primary work location / "home" site), they are to be operated in accordance with the System Security Plan for the information system.

j. Visitors bringing a portable computing device into a Property Protection, Limited, Exclusion, or Protected Area may be also be required to complete other operational or security processes or entry of the portable computing device will be denied.

k. Portable computing devices or components of portable computing devices, such as removable disk or disk drives, containing classified information must be protected and transported in accordance with Classified Matter Protection and Control requirements.

l. Portable computing devices or components of portable computing devices, such as removable disk drives, containing information in the Unclassified Protected or Unclassified Mandatory Protection information groups, as defined in Attachment 1, Chapter G, NAP 14.1-B, *NNSA Cyber Security Program*, must be protected and transported in accordance with the information they contain.

This page intentionally blank.

CHAPTER C

PASSWORD GENERATION, PROTECTION, AND USE

1. INTRODUCTION. This chapter establishes minimum criteria and processes for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified National Nuclear Security Administration (NNSA) information systems, applications, and resources. This chapter applies to any multi-user information system at a NNSA site that collects, stores, transmits, or processes unclassified or classified information and uses passwords to authenticate users or applications.

2. CRITERIA AND PROCESSES.

   a. Password Generation/Verification. Password generation or verification software must ensure that passwords are generated using the following features.

      (1) Passwords contain at least eight non-blank characters.

      (2) Passwords contain a combination of letters (preferably a mixture of upper and lowercase), numbers, and at least one special character within the first seven positions, provided such passwords are allowed by the operating system or application.

      (3) Passwords used on information systems that collect, store, transmit, or process classified information must be machine generated or use DAA-approved alternative methods of authenticating users or generating passwords.

      (4) Passwords employed by a user on unclassified information systems must be different than the passwords employed by the same user on classified information systems.

   b. Password Protection.

      (1) Passwords used to access information systems processing classified data must be protected at a level commensurate with the classification level and most restrictive category of the information to which they allow access.

      (2) Passwords used to access information systems processing unclassified data must be protected in accordance with the information with the highest level of Consequence of Loss of confidentiality or integrity on the system to which they allow access.

      (3) Passwords must not

         (a) Contain the user account identifier.

         (b) Contain any common English dictionary word, spelled forward or backwards; dictionaries for other languages may also be used if justified by risk and cost benefit analysis as documented in the approved System

Security Plan or Cyber Security Program Plan (CSPP) and referenced in the Security Plan.

(c) Employ common names, including the name of any fictional character or place, spelled forward or backwards.

(d) Contain any commonly used numbers (e. g., the employee serial number, Social Security number, birth date, phone number) associated with the user of the password.

(e) Contain any simple pattern of letters or numbers, such as “qwertyxx” or “xyz123xx.”

(4) User-generated passwords on information systems that collect, store, transmit, or process only unclassified information. If the information system user is permitted to generate his/her own password (regardless of whether the password is verified by password verification software), the user must ensure the password is consistent with the security features listed paragraph 2.a.

(5) When an information system cannot prevent a password from being echoed (e.g. in a half-duplex connection), an overprint mask must be printed before the password is entered to conceal the typed password.

(6) Individuals must not –

(a) Share passwords except in emergency circumstances or when there is an overriding operational necessity, as described in the information system's approved Security Plan or the site’s CSPP.

(b) Enable applications to retain passwords for subsequent reuse, except as described in the information system's approved Security Plan.

(c) Create his/her own passwords if the password is used for access to classified information.

c. Standard Passwords. User software, including operating system and other security-relevant software, may be supplied with standard identifiers (e.g., System, Test, and Master) and passwords already enrolled in the system. Passwords for all standard identifiers must be changed before allowing the general user population access to the information system. These passwords must be changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.

d. Password Changing. Passwords must be changed–

(1) At least every 6 months on information systems where the Consequence of Loss of confidentiality or integrity for any Information Group[1] is "Medium" or greater and at least every 12 months on information systems where the highest Consequence of Loss of confidentiality or integrity for any information group on the information system is "Low" or less;

(2) As soon as possible, but within 1 business day, after a password has been shared or compromised, or after the user suspects that a password has been compromised; and

(3) On direction from management or the DAA.

e. Administration. The information system, application, or resource where passwords are used for user authentication must, where technically feasible, ensure:

(1) Five consecutive failed attempts to provide a legitimate password for an access request results in an access lockout. The process for restoration of an account must be documented or referenced in the approved Security Plan.

(2) The user password, whether user-selected or automatically generated, is rejected if the password does not meet the criteria in this chapter.

(3) Individuals are notified that their passwords are about to expire and must be changed before expiration or lockout will occur.

(4) Any file, folder, database, or other collection of one or more user passwords is protected from access by unauthorized individuals.

(5) Periodic (e.g., monthly or quarterly) validation of conformance to password policy.

f. Clear Text Passwords. The use of clear text passwords must be eliminated from all information systems, applications, and resources.

(1) Each NNSA site's CSPP shall include a plan, with schedules and milestones, to eliminate the use of clear text reusable passwords from existing electronic information systems, and resources.

(2) Each NNSA site shall develop procedures to ensure that clear text reusable passwords are removed from new information systems, applications, and resources before the systems, applications, or resources are placed into production use.

[1] Information Groups are defined in Attachment 1, Chapter G, NAP 14.1-B, *NNSA Cyber Security Program.*

This page intentionally blank.

CHAPTER D

INFORMATION CONDITION (INFOCON)

1. INTRODUCTION. This chapter describes the minimum preparations and actions to uniformly react to warnings of cyber security incidents, heighten or reduce the cyber defensive posture, to defend against computer network attacks, and to mitigate sustained damage to NNSA information and infrastructure, including computer and telecommunications networks and systems. The INFOCON is a comprehensive defense posture and response based on the status of information systems, NNSA operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system impacts all personnel who use NNSA information systems, protects systems while supporting mission accomplishment, and coordinates the overall defensive effort through adherence to standards.

   The INFOCON system presents a structured, coordinated approach to react to adversarial attacks on NNSA information, computer systems, and telecommunication networks and systems. While all communications systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and remote access capability make computer network attack (CNA) an attractive option to an adversary. CNA is defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." INFOCON also outlines countermeasures to scanning, probing, and other suspicious activity; unauthorized access; and data browsing. NNSA INFOCON measures focus on computer network-based protective measures due to the unique nature of CNA. Each level reflects a defensive posture based on the risk to NNSA operations through the intentional disruption of information systems and networks.

2. CRITERIA AND PROCESSES.

   a. Each NNSA site's INFOCON response measures must be documented in the site's Cyber Security Program Plan (CSPP).

   b. INFOCON procedures must be well integrated with the site's Security Condition (SECON) procedures, emergency procedures, Continuity of Operations plans, and incident handling processes.

   c. Reporting of cyber security incidents must be accomplished as described in Chapter A.

   d. NNSA site managers may evaluate their situation and change the INFOCON of their organizations or site(s); however, the INFOCON must remain at least as high as the current INFOCON directed by NNSA.

   e. Local changes in the INFOCON of an NNSA site must be reported to the NNSA CSPM, through the cognizant Cyber Security Office Manager (CSOM), within 4 hours.

   f. Managers of NNSA sites must notify the CSPM, through the cognizant CSOM, if recommended or directed INFOCON response measures conflict with organization or mission priorities within 2 hours of NNSA determination of INFOCON response measures.

g. The CSPM will notify NNSA sites, through the CSOMs, when the NNSA INFOCON is changed, through the most rapid means available.

h. Site Office Directors/Managers of NNSA sites must disseminate INFOCON information within their organization and to organizations under their cognizance, through the most rapid means available.

3. NNSA INFOCON. Several critical assumptions were made about the nature of CNA and CNE in developing the NNSA INFOCON system. Understanding these assumptions is essential to effective implementation of this system.

a. Shared Risk. In today's network-centric environment, risk assumed by one NNSA site is risk shared by all. Unlike most other security activities, a successful network intrusion in one NNSA location may, in many cases, facilitate access at other locations. This necessitates a common understanding of the situation and responses associated with the declared NNSA INFOCON. These actions must be carried out concurrently at all NNSA locations for an effective defense.

b. Advance Preparation. Preparation is key, given the speed and reduced signature of CNA and CNE. Protective measures must be planned, prepared, exercised, and often executed well in advance of an attack. Preventive measures are emphasized in INFOCON responses because there may be little time to react effectively during the attack. Prevention of system compromise (see Attachment 2 for various advisories to consider) is preferable but may not be achievable.

c. Anonymity of Attacker. Attributing the attack to its ultimate source, if possible, will normally not occur until after the attack has been executed. This limits the range and type of options available to INFOCON decision makers. To effectively operate in this environment, knowledge of the adversary's identity cannot be a prerequisite to execution of defensive strategies and tactics.

d. Characterization of the Attack. Distinguishing between hacks, attacks, system anomalies, and operator error may be difficult. The most prudent approach is to assume malicious intent until an event is assessed otherwise. (See Appendix 3 for various assessments to consider.)

4. INFOCON LEVELS. The NNSA INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on NNSA information, computer systems, and telecommunication networks and systems. The NNSA INFOCON system identifies the following five levels of CNA/CNE conditions within NNSA.

Table 1. INFOCON Levels

INFOCON Level	DESCRIPTION
NORMAL	• No significant activity. • Normal operations • Network penetration or denial of service attempted with no impact to NNSA, DOE, or site operations such as Type 2 reconnaissance activity or intrusion attempts with a low impact. • Minimal attack success, successfully counteracted such as a Type 1 unauthorized use with a low impact. • General threat unpredictable
ALPHA	• Indications and warnings (I&W) indicate general threat. • Regional events occurring which affect US interests and are likely to affect NNSA interests; and involve potential adversaries with suspected or known CNA capability. • Information system probes; scans or other activities detected indicating a pattern of surveillance such as Type 2 reconnaissance activity with a moderate or high impact. • Nation- or Internet-wide computer network exploit such as a Type 1 web site defacement, malicious code, or denial of service with an impact of low. • Increased and / or more predictable threat events • Incident occurs at NNSA or DOE site
BRAVO	• I&W indicate targeting of specific system, location, unit or operation. • Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance. • Network penetration or denial of service attempted with no impact to NNSA or DOE operations such as Type 2 attempted intrusion with a low impact. • Incident occurs at NNSA site that affects an NNSA enterprise system or may impact another NNSA site such as a Type 1 compromise/intrusion with a low impact. • Intelligence indicates imminent attack against NNSA or DOE site
CHARLIE	• Intelligence attack assessment(s) indicate a limited attack. • Information system attack(s) detected with limited impact to NNSA or DOE operations: • Minimal attack success, successfully counteracted. • Few or no data or systems compromised. • Site able to accomplish mission. • Computer Network Exploit at a DOE or NNSA site such as Type 1 compromise/intrusion with low impact • Nation- or Internet-wide computer network exploit • Intelligence indicates imminent attack against national infrastructure or national security element
DELTA	• Successful information system attack(s) detected which impact NNSA operations such as a Type 1 compromise/intrusion or denial of service with a moderate or high impact. • Widespread incidents that undermine ability to function effectively. • Significant risk of mission failure. • Computer Network Attack against national infrastructure or national security element

5. INFOCON ACTIVITIES.

a. Determining the INFOCON. There are three broad categories of factors that influence the INFOCON: operational, technical, and intelligence, including foreign intelligence and law

enforcement intelligence. Some factors may fall into more than one category. The INFOCON level is based on significant changes in one or more of them. Appendix 2 describes several factors that may be considered when determining the INFOCON. The decision to change the INFOCON should be tempered by the overall operational and security context at that time. For example, an intruder could gain unauthorized access and not cause damage to systems or data. This may only warrant INFOCON ALPHA or NORMAL during peacetime, but may warrant INFOCON CHARLIE during a crisis, or it may warrant a high INFOCON at the affected site but not throughout the NNSA as a whole.

b. Declaring INFOCONs. The NNSA CSPM will recommend changes in NNSA INFOCON to the NNSA Chief Information Officer, who is responsible for declaring an NNSA INFOCON. Assimilation and evaluation of information to assess the CNA/CNE situation NNSA-wide will be a collaborative effort coordinated by the NNSA CSPM. Managers of NNSA sites are responsible for assessing the situation and establishing the proper INFOCON based on evaluation of all relevant factors (See Appendix 1 and 2 for criteria and guidance, respectively). NNSA site managers may change the INFOCON of their organizations or site(s); however, they must remain at least as high as the current INFOCON directed by NNSA. Managers changing the INFOCON of their organization or site(s) must report to the CSPM using the same reporting format described in paragraph 5.d.

c. Response Measures. Ideally, CNA/CNE operations will be based on advanced warning of an attack. Measures should be commensurate with the risk, the adversary's assessed capability and intent, and mission requirements. Over-aggressive countermeasures may result in self-inflicted degradation of system performance and communication ability, which may contribute to the adversary's objectives. Managers must also consider what impact of imposing a higher INFOCON for their organization will have on connectivity with computer networks and systems of other NNSA sites and operations. Managers will notify the CSPM, through the cognizant CSOM, if recommended or directed response measures conflict with organization or mission priorities. Regardless of the INFOCON level declared at the affected site, it is incumbent upon the affected site to report all unauthorized accesses in a timely manner in accordance with the NNSA PCSP. Each NNSA site shall have documented procedures to guide their responses and ensure these procedures are well integrated with other site SECON, emergency procedures, and Continuity of Operations plans. (See Appendix 1 for recommended action activities.)

d. Reporting. Reporting of cyber security incidents must be accomplished as described in Chapter A. However, INFOCONs assess potential and/or actual impact to NNSA operations and must be reported as follows:

(1) Reporting Channels. NNSA sites must report INFOCON changes to the NNSA CSPM and cognizant DAA through the cognizant Cyber Security Office Manager (CSOM).

(2) Reporting Frequency. NNSA sites must report INFOCON changes for their sites no later than 4 hours after the INFOCON has changed. Provide whatever information is available at the time and indicate information that is unknown or unavailable.

Information missing from the initial report will be forwarded in a follow-up report when it becomes available.

(3) Report Formats. Reports of changes in INFOCON should be accompanied by an operational assessment of the situation when appropriate. Appendix 3 outlines a process for assessing the operational impact of a CNA. Report contents shall include, as a minimum:

(a) For all INFOCONs: Organization and location, date/time of report, current INFOCON, reason for declaration of this INFOCON, response actions taken, and Point of Contact (POC) name and contact information.

(b) INFOCON BRAVO and higher. All of the above, plus: NNSA Computer Emergency Response Team (CERT) or NNSA IARC Number, (IARC will report to CIAC) and law enforcement agency (LEA) case number with POC name and contact information, when available.

(c) INFOCON CHARLIE and higher. All of the above, plus: system(s) affected (i.e. network, classification, etc.), degree to which operational functions are affected, impact (actual and/or potential) on current/planned missions and/or general capabilities, restoration priorities, and workarounds.

(4) Dissemination of NNSA INFOCON. The CSPM will send notification to NNSA sites, through the CSOMs, when the NNSA INFOCON is changed, through the most rapid means available. NNSA sites are responsible for rapid dissemination of the INFOCON information within their organization and to contractor organizations under their cognizance. Notification will include the following information:

(a) Date/time of report.

(b) Current INFOCON.

(c) Reason for declaration of this INFOCON, to include a detailed description of the causal activities to include Type and System Impact Category.

(d) Current/planned operation(s) or capabilities, units/organizations, networks, systems, applications or data assessed to be impacted or at risk.

(e) Recommended or NNSA-directed actions.

(f) References to relevant technical advisories, intelligence assessments, etc.

(g) POC information.

(h) Information that may assist sites in their response (See Appendices 2 and 3)

6. Relationship of INFOCON to Other Alert Systems. The INFOCON and Security Condition (SECON) may complement each other. The INFOCON may be changed based on the national or world situation, the intelligence community's level of concern, or other factors. Likewise, a change in INFOCON may prompt a corresponding change in other alert systems.

7. Exercises. INFOCON procedures shall be practiced in all NNSA sites as part of their self-assessment program to include operational impact assessments. (See Appendix 3).

CHAPTER E

WIRELESS TECHNOLOGIES

1. INTRODUCTION. This Chapter establishes the minimum security controls that are to be enforced by NNSA sites using wireless technologies (see definitions in Attachment 2), to ensure that security risks posed by wireless applications, devices, and network implementations are appropriately analyzed and controlled. This Chapter applies to any wireless technologies (WT) that collect, store, transmit, process, create, or disseminate unclassified or classified NNSA information. This Chapter applies to any WT lifecycle, including the development of new WT applications, the incorporation of WT into an infrastructure, the incorporation of WT outside the infrastructure, the development of prototype WT, the reconfiguration or upgrade of existing WT, and legacy systems. Land mobile radios, one-way receive-only devices, and mobile satellite services are excluded from this Chapter.

2. CRITERIA AND PROCESSES. In order to ensure that security risks posed by WT are sufficiently analyzed and appropriately controlled, NNSA sites must establish a systematic process for managing risks posed by WT and ensure the process is fully described in their Cyber Security Program Plan (CSPP). The process must:

   a. Identify the roles and responsibilities of all key personnel responsible for the decision whether to incorporate WT into the environment, including personnel responsible for telecommunications, TEMPEST, Protected Transmission Systems (PTS), and Technical Surveillance Countermeasures (TSCM) program compliance.

   b. Evaluate the business needs for deploying WT, to include cost/benefit analysis and whether more secure technologies (e.g., expansion of wired network) are feasible.

   c. Include a risk assessment to evaluate the risks to the confidentiality, integrity, and availability of site information resources in the context of wireless networking devices to include the entire spatial volume of transmitted/received signal capability. (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, dated November 2002 may be used to assist in decision-making).

   d. Evaluate the planned wireless networking applications with respect to specific WT, physical location on site, proximity to sensitive or classified information processing areas, connectivity of wireless devices to site computers and networks, and the Information Groups and information systems connected to WT.

   e. Identify the specific security mechanisms implemented through technical, operational, and configuration management controls that will ensure risk is maintained at an acceptable level and the schedule for testing such controls to ensure they operate as intended. At a minimum, these controls must:

(1) Address the procurement standards, intrusion detection and vulnerability scanning capabilities, minimum security configurations, monitoring for fraud, waste, or abuse, as well as specific training on individual rules of behavior and consequences for rule violation for cyber security personnel, network administrators, and users.

(2) Address the Protection Profile requirements for the Information Group(s) intended for processing with WT.

(3) Require labeling, inventorying, and registration of any fielded WT access points and clients.

(4) Require semi-annual performance reviews to ensure accuracy of access point inventory, security of configurations, or identification of unauthorized devices.

(5) Require proper installation and physical control of all access points.

(a) Ensure NIC and access point firmware is up-to-date.

(b) Ensure only authorized people can reset the access points.

(c) Assign strong passwords (in accordance with Chapter III) to access points. In addition, access points must be administered via the site's wired network or locally via the access point's built-in COM ports.

(d) Utilize static IP addresses for clients and access points.

(e) Ensure the capability to detect transmissions by unauthorized access points and/or WT clients is in place and operational prior to authorized use.

(6) Require regular application of patches and security enhancements.

(7) Adopt strong encryption methods that encompass end-to-end encryption of information as it passes throughout the wireless network. Use a Type I product to encrypt transmission of information to/from National Security Systems. Use Type II or III products to encrypt transmission of information to/from non-National Security Systems.

CHAPTER F

REMOTE ACCESS

1. INTRODUCTION. Remote access is defined as accessing an information system (at the system level or application level) from a location outside the confines of a network as defined in each site's Cyber Security Program Plan.[2] Remote access to NNSA information and systems can promote cost-effective benefits to the NNSA mission and workforce. At the same time, remote access can introduce significant risk to those systems. Federal law and implementing policies require agencies to develop, document, and implement programs to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support agency operations and assets. The remote system may not have been evaluated through the NNSA PCSP C&A process therefore its security policy is unknown. Based upon documented risk assessments, agencies must provide adequate security to maintain an acceptable level of risk to agency operations and assets.

2. CRITERIA AND PROCESSES.

   a. All NNSA sites must develop and implement policies, processes, and procedures to govern remote access of NNSA information systems by users utilizing NNSA and non-NNSA owned equipment. These processes and procedures are documented as part of the Sites' CSPP (see NAP 14.1-B, Attachment 1, Chapter F). All policies, processes, and procedures must address the following:

      (1) Use of Government- and non-Government-owned computers to remotely access NNSA information resources or information.

      (2) The protection of information on non-Government-owned computers.

      (3) The prohibition by the Department of Commerce of export from the United States of any encryption program or algorithm in excess of 128 bits.

      (4) The prohibition of the importation and use of certain encryption standards by certain foreign governments.

      (5) System Security Plan (SSP) modifications when remote access capabilities are to be introduced into legacy applications or systems.

      (6) National Security Systems. Remote access to any DOE/NNSA National Security System is authorized via approved methods (e.g., SecureNet, etc.) with Type I

[2] This Chapter does not address risks associated with or the criteria and processes specific to wireless networks and devices. The criteria and processes for these are addressed in Chapter E.

encryption. NNSA and NNSA contractors and subcontractors will ensure that only personnel with the access authorization and need-to-know can access National Security Systems. The risk associated with remote access shall be documented in the relevant System Security Plan. Personnel accessing these systems shall be trained and the training shall be documented.

(7) Management Controls on Remote Access must describe:

(a) Boundary Protection Services and automated tools (e.g., firewalls, virtual private networks, encryption, intrusion detection, anti-virus software, and audit log analysis) provided to manage remote access services and detect intrusions and/or intrusion attempts in addition to those required in the NNSA Program Cyber Security Plan (PCSP).

(b) Procedures to report and respond to remote access security incidents.

(c) Two-factor authentication where one of the factors is provided separate from the computer gaining access (i.e. RSA token or your finger, in a biometric solution).

(d) Time-out function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity.

(e) Procedures to conduct random security evaluations of remote access controls for all Information Groups described in NAP 14.1-B, Attachment 1, Chapter G, and systems used to remotely access NNSA information in all Information Groups, except the Open Public Access Information Group.

(f) Rules of behavior and operations and consequences for violating remote access policy and procedures, including the prohibition of entering any classified information on any computing resource not approved for such information.

(g) Specific security and awareness training for those authorized to use remote access services to access information in all Information Groups described in NAP 14.1-B, Attachment 1, Chapter G, except the Open Public Access Information Group, and those who perform system administration duties.

(h) Process(es) to perform a risk assessment if new threats are introduced by allowing remote access to NNSA information and systems (including trusted and non-trusted environments).

(i) Procedures to ensure that management’s initial and periodic approval of the operational need of each user’s remote access capability is obtained.

(j) Procedures to ensure NNSA systems are protected from malicious code on equipment used for remote access.

(k) Process for organizations and users to obtain approval from system owners and data custodians prior to implementing remote network access.

(l) Processes to ensure that remote access services are controlled and that user profiles are managed to reflect user job responsibilities.

(m) Processes to ensure periodic reviews of remote access security controls.

(n) Processes to ensure that remote access issues, vulnerabilities, requirements, and technology changes are incorporated into training for all affected NNSA and contractor personnel, including, as appropriate, the permitted extent of personal use.

(o) Remote access requirements in the SSP MOA/SIA of the TOE being accessed remotely.

(8) Operational Controls on Remote Access must describe:

(a) The minimum requirements for operating system and application software for users who use non-NNSA-owned equipment to connect remotely to NNSA networks for access to all Information Groups described in NAP 14.1-B, Attachment 1, Chapter G, except the Open Public Access Information Group.

(b) Procedures for obtaining user commitment to understanding and acknowledgement of minimum requirements and remote access rules of behavior through user signatures on a User Responsibility Statement that includes the requirements for remote access.

(9) Technical Controls. Develop or define and describe the following:

(a) Acceptable levels and types of authentication, and personal identification for remote access.

(b) Establishment of a trusted path prior to the transmission of data in all Information Groups described in NAP 4.1-B, Attachment 1, Chapter G, except the Open Public Access Information Group.

(c) Minimum requirements for the operating system and application software and for controlling and safeguarding Government-issued cryptographic keying material on all equipment used for remote access.

(d) Standard minimum security configurations for all information systems.

(e) Procedures to ensure currency of updates of security-related software patches and/or hardware updates on remote equipment prior to granting access to all Information Groups described in NAP 14.1-B, Attachment I, Chapter G, except the Open Public Access Information Group.

(f) An asset management infrastructure for compilation, collection, and reporting of vulnerability assessment and remediation, information technology assets, compliance with configuration standards, and management of information system patches.

b. Significant Changes. Owners and operators of interconnected applications and systems must be apprised of any significant change to interconnection agreements. Any Site's application or system that uses remote access for which the above criteria are not met must be documented as a weakness in applicable corrective action plans and milestones.

APPENDIX 1

RECOMMENDED ACTIONS

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
NORMAL	• No significant activity. • Normal operations • General threat unpredictable	• Ensure all mission critical information and information systems (including applications and databases) are identified • Ensure all points of access and operational necessity are identified • On a continuing basis, conduct normal cyber security practices • Periodically review and test higher INFOCON actions
ALPHA	• Indications and warnings (I&W) indicate general threat. • Regional events occurring which affect US interests and involve potential adversaries with suspected or known CNA capability. • Information system probes; scans or other activities detected indicating a pattern of surveillance. • Increased and / or more predictable threat events • Nation- or Internet-wide computer network exploit. • Incident occurs at NNSA or DOE site • Intelligence indicates imminent attack against NNSA or DOE	Accomplish all actions at INFOCON Normal, plus the following • Execute appropriate cyber security practices • Heighten user awareness • Execute appropriate defensive actions • Follow NNSA reporting procedures identified in NNSA cyber security policies • Review higher INFOCON actions • Consider proactive execution of some, or all, higher INFOCON actions

BRAVO	• I&W indicate targeting of specific system, location, unit or operation.
	• Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance.
	• Network penetration or denial of service attempted with no impact to NNSA or DOE operations.
	• Incident occurs at NNSA site that affects an NNSA enterprise system or may impact another NNSA site.
	• Intelligence indicates imminent attack against NNSA or DOE site
		Accomplish all actions at INFOCON Alpha, plus the following
		• Execute, as appropriate, the following cyber security practices (recommended practices in NNSA cyber security policies)
		  ◦ Increase level of auditing on critical systems
		  ◦ Immediately review for security, and patch, as needed, all critical systems
		  ◦ Consider limiting connections and traffic that cross site perimeter
		• Isolate compromised systems immediately
		• Follow NNSA reporting procedures identified in NNSA cyber security policies
		• Review higher INFOCON actions
		• Consider proactive execution of some, or all higher INFOCON actions

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS

CHARLIE	• Intelligence attack assessment(s) indicate a limited attack.
	• Information system attack(s) detected with limited impact to NNSA or DOE operations:
	• Minimal attack success, successfully counteracted.
	• Few or no data or systems compromised.
	• Site able to accomplish mission.
	• Computer Network Exploit at a DOE or NNSA site
	• Nation- or Internet-wide computer network exploit
	• Intelligence indicates imminent attack against national infrastructure or national security element
		Accomplish all actions at INFOCON Bravo, plus the following
		• Execute, as appropriate, the following cyber security practices (recommended practices in NNSA cyber security policies)
		  • Increase level of auditing on critical systems
		  • Minimize connections and traffic to absolute minimum needed for current mission operations
		  • Reconfigure systems to minimize access points and increase security
		  • Consider disconnecting all non-mission-critical systems and networks from the Internet
		• Isolate any compromised systems immediately
		• Follow NNSA reporting procedures identified in NNSA cyber security policies
		• Review higher INFOCON actions
		• Consider proactive execution of some, or all, higher INFOCON actions

DELTA	• Successful information system attack(s) detected which impact NNSA operations.
	• Widespread incidents that undermine ability to function effectively.
	• Significant risk of mission failure.
	• Computer Network Attack against national infrastructure or national security element
		Accomplish all actions at INFOCON Charlie, plus the following
		• Execute, as appropriate, the following cyber security practices (recommended practices in NNSA cyber security policies)
		  • Designate and reconfigure information systems and networks to use controlled connections and traffic
		  • Execute procedures for ensuring graceful degradation of information systems and network(s)
		  • Disconnect all non-mission-critical systems and networks from Internet.
		  • Implement procedure for 'stand-alone" or manual operations
		• Follow NNSA reporting procedures identified in NNSA cyber security policies
		• Execute applicable portions of Continuity of Operations plans

APPENDIX 2

FACTORS INFLUENCING THE INFOCON

When determining the appropriate defensive posture, many factors must be considered. This appendix lists several factors that managers should consider when determining the INFOCON. (Note: This list is offered as broad guidance; other factors may also be considered.)

- Other indications & warning (including domestic threats). NSA IPC Alerts; National Infrastructure Protection Center (NIPC) advisories, threats, warnings; law enforcement agency intrusion reports, etc.
- CNA intelligence assessments.
- Current world situation. Increased tensions with a nation possessing CNA capability may precede CNA operations against us.
- Other alert systems such as SECON, etc. Managers must determine if a change in one alert status will cause a corresponding change in another alert status.
- Dependence of NNSA functions upon particular information systems. This type of analysis may suggest the degree to which a particular network, system, application or database is mission critical.
- Manager's assessment of mission-critical information system readiness. This readiness may be determined from the networks' security posture, vulnerability, extent of compromise, etc.
- Manager's assessment of readiness to coordinate the protection of critical infrastructure and key resources identified under Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*
- Incident reports. These are roughly analogous to attack assessment.
- Trend analyses. Reports showing number, type, and frequency of attacks, systems targeted, hot IP addresses, etc.
- Technical impact assessment. This information may be included in an incident report or may result from follow-on analysis. This assessment may include the extent of system compromise and/or disruption and the degree to which system confidentiality, integrity, availability, and authentication have been affected.
- Operational impact assessment--a key element in determining the INFOCON. (See Appendix 3.) The process for assessing operational impact also lays the groundwork for executing preventive measures, developing workarounds, and establishing restoration priorities.

- Manager's assessment of the potential for an information attack. Although much objective data is available on which to base the decision, the final judgment for declaring an INFOCON change rests with the manager. Objective assessment of the situation and prudent analysis of all available information must be integrated with the manager's experience and leadership to determine the organization's appropriate defensive posture.

APPENDIX 3

OPERATIONAL IMPACT ASSESSMENT

Assessing the impact of CNE/CNA on our ability to conduct operations is key to conducting damage assessment, prioritizing response actions, and assisting in identifying possible adversaries. This appendix offers an operational impact assessment process that may be used when reporting changes in INFOCON. Note: Assessment results are classified SECRET at a minimum. The assessment process itself is unclassified.

Prior to an attack:

- Identify all critical information systems.
- For each critical information system, identify all resident critical applications and databases.
- Determine which NNSA functions are supported by each application/database

After an attack or attempted attack has been detected:

- Identify all critical information systems that are, or appear to be, targeted.
- For each information system targeted, determine the technical impact, i.e., to what degree are confidentiality, integrity, availability, and authentication affected? What critical applications and databases are impacted?
- For the technical impacts identified, estimate the time and resources required to restore functionality. Identify any interim workarounds.
- How does the technical impact of the attack affect the organization's ability to function?
- How does the impact to the organization's ability to function affect support to current/projected operations? If no specific operations are ongoing or projected, how is general capability/readiness affected?

This page intentionally blank.

ATTACHMENT 2

DEFINITIONS

CIAC	Computer Incident Advisory Capability – located at Lawrence Livermore National Lab, Livermore, CA.
Cyber Security Incident	A cyber security incident is any adverse event caused by an outsider or an insider that threatens the security of information resources. Adverse events may include compromises of integrity, denial-of-service attacks, compromises of confidentiality, loss of accountability, or damage to any part of the system. Examples include the insertion of malicious code (e.g., viruses, Trojan horses, or back doors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.
End-to-End Encryption	Encryption of information at its origin and decryption at its intended destination without intermediate decryption.
IARC	NNSA Information Assurance Response Center (IARC) – Located in Las Vegas, NV. 702-942-2611
Land Mobile Radio	Conventional portable systems that dedicate a single radio channel to a specific group of users who share it. These portable communication devices typically operate at the following frequency bands: very high frequency (VHF) low band, VHF high band, and ultrahigh frequency (UHF). Adjacent channel spacing is typically 20 kilohertz (kHz) for low band; 12.5, 25, or 30 kHz for high band; and 12.5 or 25 kHz for UHF.
Mobile Satellite Systems (MSS)	Networks of communications satellites intended for use with mobile and portable wireless telephones or computing devices. There are three major types: AMSS (aeronautical MSS), LMSS (land MSS), and MMSS (maritime MSS). A connection using MSS is similar to a cellular link, except the repeaters are in orbit around the earth rather than on the surface. MSS repeaters can be placed on geostationary, medium earth orbit, or low earth orbit satellites. Provided there are enough satellites in the system, and provided they are properly spaced around the globe, a MSS can link any two wireless devices at any time, no matter where in the world they are located. MSS systems are interconnected with land-based cellular networks.

Multi-user System — A system, that under normal operations has more than one user accessing it simultaneously. Systems accessed by more than one user sequentially (i.e., by one user at a time) without undergoing the necessary procedure to remove residual data between users are also considered multi-user systems.

One-way Receive Only Device

Device with a wireless receiver and no transmitter. The device is not capable of transmitting any Wireless RF (i.e., there is no wireless communication between the device and any base station, not even station keeping or "keep alive" signals.)

Personally Owned — An item that is owned by an individual and is intended solely for his/her personal use.

Personally Identifiable Information (PII)

Personal information that is associated to an individual such as social security number; place of birth; date of birth; mother's maiden name; biometric records (i.e., fingerprint, Iris scan, DNA); medical history (i.e., previous diseases, metric information, weight, height, BP); criminal history; employment history (i.e., ratings, disciplinary actions); financial information (i.e., credit card numbers, bank account numbers); and security clearance history.

WHAT IS PII:

1. Social Security Numbers in any form are PII
2. Place of Birth associated with an individual
3. Date of Birth associated with an individual
4. Mother's maiden name associated with an individual
5. Biometric record associated with an individual
    a. Fingerprint
    b. Iris scan
    c. DNA
6. Medical history information associated with an individual
    a. Previous diseases
    b. Metric information
    c. Weight
    d. Height
    e. BP
7. Criminal history associated with an individual
8. Employment history associated with an individual
    a. Ratings

   b. Disciplinary actions
9. Financial information associated with an individual
   a. Credit card numbers
   b. Bank account numbers
10. Security clearance history or related information

WHAT ISN'T PII:

1. Phone numbers (Work, home, cell)
2. Street addresses (Home, work, other)
3. Email addresses (Work or personal)
4. Digital pictures
5. Birthday cards
6. Birthday emails
7. Grade and Step information for Federal Employees
8. Medical Information pertaining to work status (X is out sick today)
9. Medical information included in a health or safety report (X broke his arm when…)
10. Resumes unless it includes SSN
11. Job titles for employment history, resume, or written biography
12. Federal salaries
13. Federal bonuses
14. Written biographies (like the ones used in pamphlets of speakers)
15. Alma Mater or degree level in biographies
16. Personal information stored by individuals on their personal workstation or laptop (unless a SSN)

Portable Computing Device	Portable Computing Devices are any portable devices that provide the capability to collect, create, process, transmit, store, and disseminate information. These devices include (but are not limited to) Personal Digital Assistants (PDAs), palm tops, hand-held or portable computers and workstations, non-web-enabled cell phones, web based enhanced cell phones, two-way pagers, and wireless e-mail devices.
Reusable Password	A data item associated with a user identifier that remains constant and is used for multiple access requests over some explicit time interval.

Site	An NNSA facility: can be a NNSA Service Center, NNSA Site Office, NNSA contractor or subcontractor facility, or the NNSA Headquarters activity that has a responsibility to protect NNSA information systems. It has a set of geographical boundaries as defined in a NNSA SSSP or SSP.
Special Character	Any non-alphanumeric character.
Target of Evaluation (TOE)	An IT product or information system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE Component	One or more major subsystems of the Target of Evaluation. Usually described in a Security Target as part of an SSP.
Trusted Path	Means by which a user and a TOE Security Function (TSF) can communicate with necessary confidence to support the TOE Security Policy (TSP).
Type I Product	Classified or controlled cryptographic item endorsed by the National Security Agency (NSA) for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products and not to information, key, services, or controls. Type I products contain approved NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulations.
Type II Product	Unclassified cryptographic equipment, assembly, or component endorsed by the NSA for use in National Security Systems as defined in Title 40 U.S.C. Section 1452.
Type III Product	A product using a cryptographic algorithm registered by the National Institute of Standards and Technology (NIST) and published as a Federal Information Processing Standard (FIPS) for use in protecting unclassified sensitive information or commercial information.
User	An individual who can receive information from, input information to, or modify information on an information system without an independent human review. In a processing context, this also includes a process acting on behalf of a user.

Wireless Technology	The term “Wireless Technology” (WT) is used to mean any WT that is used to collect, create, process, transmit, store, or disseminate data processed by, for, or on behalf of NNSA or DOE (excludes tactical radios and land mobile; emergency; and one-way receive-only devices). WT is defined as any device that enables communication without physical connections-without requiring network or peripheral cabling. Such technologies use radio or infrared frequency transmissions as the means for transmitting data, whereas wired technologies use cables.