National Nuclear Security Administration

Policy Letter: NAP-14.2

Date: September 12, 2003

TITLE: Baseline Cyber Security Requirements

1. OBJECTIVES.

   a. Establish requirements and responsibilities for reporting and responding to 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.

2. 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 Elements. NNSA Headquarters Organizations, Service Center, Site Offices, NNSA contractors, and subcontractors are, hereafter, referred to as NNSA elements.

   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 life cycle, 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," 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 Chapter VIII, NAP-14.1, *NNSA Cyber Security Program*.

d. 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.

e. 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 N 471.3, *Reporting Incidents Of Security Concern).*

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

4. REQUIREMENTS.

a. The requirements and responsibilities for reporting and responding to cyber security incidents involving NNSA information systems are defined in Chapter I.

b. The requirements 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 II.

c. The requirements for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified NNSA information systems, applications, and resources are defined in Chapter III.

d. The requirements and guidance for standardized procedures and responsibilities for authorizing and communicating Information Conditions (INFOCONs) throughout the NNSA are defined in Chapter IV.

5. CONTACT. Questions concerning this NAP should be directed to the NNSA Cyber Security Program Manager at 202-586-4775.

6. DEFINITIONS. See Attachment 5.

BY ORDER OF THE ADMINISTRATOR:

Linton Brooks
Administrator

Attachments

This page intentionally blank.

CHAPTER I

REPORTING AND RESPONDING TO CYBER SECURITY INCIDENTS

1. INTRODUCTION. This chapter establishes the requirements and responsibilities for reporting and responding to cyber security incidents involving NNSA information systems.

2. REQUIREMENTS.

   a. Reportable Cyber Security Incidents. All NNSA elements must develop and document, in their Cyber Security Program Plan (CSPP), processes for reporting cyber security incidents. NNSA elements must report cyber security related incidents that meet one or more of the following criteria:

      (1) Incidents of Security Concern. Report the cyber security aspects of the following Incidents of Security Concern, as adapted from DOE N 471.3, *Reporting Incidents Of Security Concern.*

         (a) 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 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 N 471.3.* These incidents must be reported within 1 working hour of discovery.

            - Confirmed or suspected loss, theft, or 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.

         (b) Impact Measurement Index (IMI-2). Reports incidents that pose a near- or long-term threat to national security interests and/or critical NNSA or Department of Energy 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 the reporting requirements in DOE N 471.3.* 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 3, NAP-14.1, *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.
- Confirmed or suspected unauthorized disclosure, loss/potential loss of Unclassified Mandatory Protection Information (as defined in Attachment 3, NAP-14.1, *NNSA Cyber Security Program*) via intrusions, hacking, or break-ins into NNSA information systems or loss/potential loss of cyber media.

(c) Impact Measurement Index (IMI-3). Report incidents that pose long-term threats to Department of Energy 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 the reporting requirements in DOE N 471.3*. 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.

(2) Incidents of NNSA Cyber Security Concern. These incidents must be reported within eight- (8) working hours of discovery.

(a) Unauthorized Access. Report all unauthorized, successful accesses, in particular root or administrator compromises, and all unsuccessful attempts of unauthorized access if there is reason to suspect the attempts are related to previous attempts, are significant, or are unusually persistent.

(b) Denial-of-Service. Report any denial-of-service (successful or unsuccessful) event that affects a critical service, such as, e-mail, primary web, Internet web, router or switch, DNS, etc., or denies access to all or a large portion of a NNSA element's network.

(c) Reconnaissance Scans, Probes, Attempted Denial-of-Service. Report all unauthorized network scans/probes/attempted denial-of-service, if there is reason to

suspect that the scans are related to previous attempts, are significant, or are unusually persistent.

(d) Impact on Multiple NNSA Elements. Incidents, not including contamination of unclassified information systems with classified information, with the potential to (or which actually do) affect other NNSA elements.

(e) Malicious Code. Report all instances of viruses, Trojan Horses, or worms that either (a) infected one or more hosts at a site and caused significant impact on programmatic mission or (b) have not been seen before. Malicious code detected and blocked by commercial e-mail proxies or similar mechanisms do not need to be reported unless it occurs in significant numbers or meets the criteria of section 2.a.(1).

(f) Alleged Criminal Activity. Report all instances alleging criminal activities involving cyber resources. These types of activities are outlined in DOE N 221.8, *Reporting Fraud, Waste, and Abuse*.

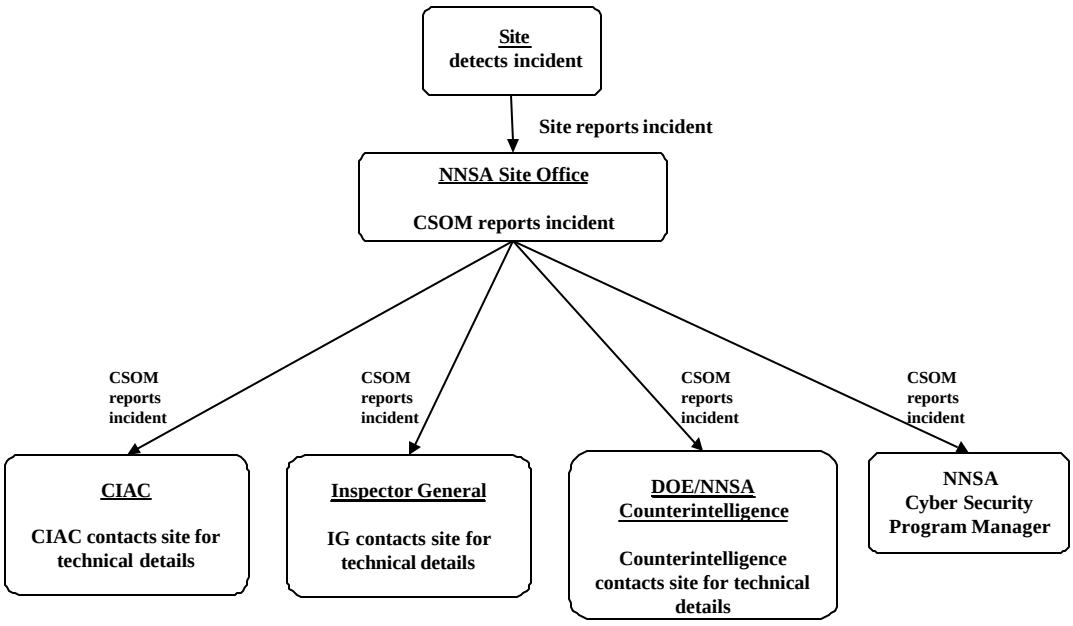

Figure 1. NNSA Cyber Security Incident Reporting Process

b. Cyber Security Incident Reporting Protocol. Figure 1 illustrates the process for reporting NNSA cyber security incidents.

(1) The cognizant Cyber Security Office Manager (CSOM) must be notified, within the time period identified in section 2.a, of all reportable cyber security incidents, identified in section 2.a, after discovery by the NNSA element.

(2) The cognizant CSOM must report to the NNSA CSPM, within eight- (8) working hours after notification by the NNSA element, incidents or activities if there is reason to suspect that the incidents are significant, possibly affect multiple NNSA elements, or are unusually persistent, and incidents listed in paragraph 2.a.(2) above.

(3) The CSOM must notify the DOE Computer Incident Advisory Capability (CIAC), within eight (8) working hours, after receiving an incident report from an NNSA element. Requiring the CSOM To notify CIAC could cause an unnecessary delay in the reporting and possible solutions provided by CIAC. In addition, the CSOM may not have all the technical information required to provide a meaningful report to CIAC. Recommend this be revised to state the CSSM must notify CIAC.

(4) Cyber Security Incident Report Content. The cognizant CSOM will specify report content and may specify format. At a minimum, incident reports (as defined in paragraph 2.a) 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.

(5) 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.

(6) Counterintelligence Reporting. Events identified in DOE N 5670.3, *Counterintelligence Program,* must be reported by the CSOM to the Office of Counterintelligence in accordance with the reporting procedures in DOE N 5670.3.

CHAPTER II

PERSONAL ELECTRONIC DEVICES AND PORTABLE COMPUTERS

1. INTRODUCTION. 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 National Nuclear Security Administration (NNSA) and all organizations under its cognizance. These requirements apply to any portable computing device (see definition in Attachment 4) 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. REQUIREMENTS.

   a. Visitors to any NNSA Property Protection, Limited, Exclusion, or Protected Area must be advised, prior to entry, of the requirements of this policy.

   b. **Personally owned** portable computing devices:

      (1) Are prohibited from use within any NNSA Property Protection, 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 element'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 element's CSPP;

      (4) Are prohibited from storing, processing, receiving, or transmitting classified information; and

      (5) 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 element'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) Comply with applicable National Telecommunications and Information Administration (NTIA) and Federal Communication Commission (FCC) requirements;

(5) Comply 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.

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 element's CSPP.

e. The administrative and physical controls, including TEMPEST, used to reduce the risks from the use of any portable computing devices must be documented in the element'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 element portable computing device procedures. The responsible supervisory personnel must take disciplinary action in accordance with the NNSA element'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 element's CSPP. The cognizant Designated Approving Authority (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 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 required to meet additional requirements 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 3, NAP-14.1, *NNSA Cyber Security Program*, must be protected and transported in accordance with protection requirements for the sensitive information they contain.

This page intentionally blank.

CHAPTER III

PASSWORD GENERATION, PROTECTION, AND USE

1. INTRODUCTION. Establish minimum requirements 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. These requirements apply 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. REQUIREMENTS.

   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 protection requirements for 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 element'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 12 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 requirements in this NAP.

(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'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 in the NNSA element CSPP.

---

[1] Information groups are defined in NAP-14.1, *NNSA Cyber Security Programs*.

(2) Each NNSA element 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.

CHAPTER IV

INFORMATION OPERATIONS CONDITION (INFOCON)

1. INTRODUCTION. This Information Operations Condition (INFOCON) policy defines actions to uniformly 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. REQUIREMENTS.

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

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

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

   d. The NNSA Cyber Security Program Manager (CSPM) will evaluate CNA/computer network exploitation (CNE) situations NNSA-wide and recommend changes in NNSA INFOCON to the NNSA Defense Nuclear Security Chief.

   e. NNSA element 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.

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

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

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

i. Site Office Directors/Managers of NNSA elements 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 element 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 Attachment 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.

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.
	  • Minimal attack success, successfully counteracted.
	• 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. • Nation- or Internet-wide computer network exploit . • 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. • 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
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
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

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. Attachment 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 Defense Nuclear Security Chief, 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 elements are responsible for assessing the situation and establishing the proper INFOCON based on evaluation of all relevant factors (See Attachment I and IV for criteria and guidance, respectively). NNSA element 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 using the same reporting format described in paragraph 5.d the change to the CSPM using the same reporting format described in paragraph 5.d.

c. Response Measures. Response measures associated with INFOCONs are the recommended actions (unless specifically otherwise directed by NNSA). 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 elements 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 element 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 Attachment 1 for potential response activities.)

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

must be reported through operational channels. Additional INFOCON reporting requirements include:

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

(2) Reporting Frequency. NNSA elements 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. Report 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. Attachment 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 DOE Computer Incident Advisory Capability (CIAC) incident number 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 elements, through the CSOMs, when the NNSA INFOCON is changed, through the most rapid means available. NNSA elements 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.

(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 Attachments 2 and 4)

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 elements as part of their self-assessment program to include operational impact assessments. (See Attachment 3).

ATTACHMENT I

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 • 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.
		Accomplish all actions at INFOCON Alpha, plus the following
		• Execute 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 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 all 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 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

Attachment 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.
- 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 Attachment 3 for procedures.) 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.

ATTACHMENT 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?

ATTACHMENT 4

DEFINITIONS

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.
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.
Portable Computing Device	Portable Computing Devices are any portable devices that provides 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.
Special Character	Any non-alphanumeric character.
Wireless	Technology that permits the transfer of information between separated points without physical wire connection. Currently wireless technologies

	use infrared (IR) and radio frequency (RF) but, as technology evolves, wireless could include other methods of transmission.
W-IS	Wireless-Information System: Any NNSA or NNSA element wireless telecommunication or computer-related equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. W-IS includes end-systems, user devices, and technologies such as, but is not limited to, Personal Digital Assistant (PDAs), Blackberry (WGW – May need to remove this since it is a brand name), 3G Cellular Telephones, Interactive TV, Wireless/IR Copiers and Faxes, and transport infrastructure components such as, but not limited to, transmitters, receivers, amplifiers, and antennas. W-IS excludes emergency, tactical radios, and one-way receive-only devices.