CNSS-079-07
August 2007

FREQUENTLY ASKED QUESTIONS (FAQ) ON INCIDENTS AND SPILLS

Prepared By: INVESTMENT IN DETECTION, RESPONSE, AND RECOVERY TECHNOLOGY (IDRRT) WORKING GROUP

NATIONAL SECURITY SYSTEMS

Question #1: What is a "national security system" (NSS)?

A: Title 44, U.S. Code Section 3542 (b)(2), Federal Information Security Management Act (FISMA), Title III, Public Law 107-347, December 17, 2002, defines a "national security system" as follows:

(A) Any information system (including any telecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, the function, operation, or use of which:

I. Involves intelligence activities;
II. Involves cryptologic activities related to national security;
III. Involves command and control of military forces;
IV. Involves equipment that is an integral part of a weapon or weapon system; or
V. Subject to subparagraph (B [provided below]), is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Additionally, while all classified systems are NSS, not all NSS are classified or necessarily warrant the same level of protection. Further, routine administrative and business applications, as noted in subparagraph (B) above, pertaining to intelligence, cryptologic, or military force or weapons qualify as NSS.

Question #2: Who determines whether an information system is an NSS?

A: Committee on National Security Systems (CNSS) Policy No. 6, *National Policy on Certification and Accreditation of National Security Systems*[1]*,* October 2005 states "All federal government departments and agencies[2] shall establish and implement programs that mandate the certification[3] and accreditation[4] of NSS under their operational control." A

[1] Supersedes NSTISS Policy No. 6, "National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems," dated 8 April 1994.

[2] Nothing in CNSS Policy No. 6 alters or supersedes the existing authorities of the Director of National Intelligence.

[3] Certification: Comprehensive evaluation of the technical and non-technical security safeguards of an information system (IS) to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

[4] Accreditation: Formal declaration by a Designated Accrediting Authority (DAA) that an information system (IS) is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. *(C&A Working Group definition.)*

"Primary Accrediting Authority" (PAA) or "Designated Accrediting Authority" (DAA) is authorized to accredit a system. Based on the above reference, the organization's PAAs or DAAs[5] can designate a system as a NSS provided the system meets the criteria outlined in Title 44, U.S. Code Section 3543(b)(2), Federal Information Security Management Act, Title III, Public Law 107-347, December 17, 2002.

Question #3: Has any system been specifically designated as a NSS?

A: Yes. As an example, the Director, Central Intelligence Agency (CIA) has designated that all CIA systems are NSSs.

Question #4: Is there a list of NSSs?

A: None that could be identified. While it is possible that some organizations have such a list, the existence of any official or unofficial list has not been publicized.

Question #5: If individual organizations identify a NSS, who is going to maintain the comprehensive list or database?

A: No comprehensive list or database of NSS exists. However, it is recommended that individual organizations maintain a list or database of their own NSS. The Department of Defense (DoD) maintains a database called the DoD Information Technology (IT) Portfolio Repository (DIPTR) for collecting and maintaining DoD registry for FISMA, including identification of a system as a NSS.

Question #6: Are all NSSs located in government facilities?

A: No. There are NSSs located in contractor facilities that operate at various classification levels and are operated by the contractor staff for the U.S. Government.

Question #7: Can the term *NSS* be considered equivalent to *Sensitive Compartmented Information* (SCI) systems? If not, is it equivalent to a reference to "any system that process classified information"?

A: No. NSS can be deployed at any classification-level provided the system satisfies the definition provided above. Therefore, incidents can occur on or be caused from any such system. Many DoD systems are NSS systems. DoD command and control systems can be NSS even if they process only unclassified data. While all classified systems are NSS, not all NSS are classified or necessarily warrant the same level of protection. Further, routine administrative and business applications, as noted in subparagraph (B) above, pertaining to intelligence, cryptologic, or military force or weapons qualify as NSS.

[5] PAAs and DAAs include Federal Department Secretaries, Agency Heads, and the Directors of IC organizations. DAA authority can be delegated to subordinates through formally signed memoranda.

Question #8: When we discuss incidents occurring on NSSs, are we using commonly defined terms?

A: CNSS Instruction No. 4009, *"National Information Assurance (IA) Glossary,"* revised June 2006, contains all definitions pertinent to NSS IA.

- A **security event** is an occurrence, not yet assessed, that may affect the confidentially, integrity or availability of an information system processing national security information.
- A **security incident** is an assessed *event* deemed to have actual or potential adverse effects on the confidentially, integrity or availability of an information system processing sensitive information.
- A **data spill** is a security incident that results in the transfer of classified or sensitive (for example, privacy, contract sensitive) information to unaccredited and unauthorized information systems, applications or media.

  Additionally, the term data spill pertains to classified or sensitive information that is stored on or transmitted on information systems or networks that are:

  - Not formally accredited to host or process that information (e.g., SCI to Secret Internet Protocol Router Network (SIPRNET), SIPRNET to Non-secure Internet Router Network (NIPRNET)).
  - Not formally accredited to host or process information subject to specific restricted handling caveats (e.g., Proprietary Information (PROPIN), Originator Controlled (ORCON), North Atlantic Treaty Organization (NATO)).
  - Not formally accredited to host or process information under the control of a particular dissemination control system (e.g., Hybrid Control System (HCS)).
  - The inappropriate release of information to a foreign nation's IS.

- **Inadvertent disclosure** is the accidental exposure of classified or sensitive information to a person not authorized access.
- **Unauthorized disclosure** is the intentional exposure of classified or sensitive information to individuals not authorized to receive it.
- **Information owner** is the official with statutory or operational authority for specific information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
- **Data** is numbers, characters, images, sounds, or other representation of potential information, regardless of the recording medium, in a form that can be assessed by a human or (especially) input into a computer, stored and processed there, or transmitted on some digital channel. Computers nearly always represent data in binary. Data on its own has no meaning, only when interpreted by some kind of data processing system does it take on meaning and become information.
- **Information** is knowledge gained through the study, communication, research, instruction, etc. of data. For purposes of the FAQ, data and information are used interchangeably.

Question #9: What are *"intelligence systems"?*

A: Intelligence systems include all systems and networks under the purview of the Director of National Intelligence (DNI). Intelligence systems do not include collateral information systems solely because they store or process SAMI Sources And Methods Involved (SAMI) information [as documented in Director, Central Intelligence Directive (DCID) 6/5].

Question #10: What is *"intelligence information"?*

A: Intelligence information, often not differentiated from intelligence data, is any information or data under the purview of the DNI. It is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas, or, information and knowledge about an entity, often an adversary, obtained through observation, investigation, analysis, or understanding. This designation could also be applied to metadata about the information (e.g., system name, location, system mission).

Question #11: Are all intelligence systems NSSs?

A: Yes.

Question #12: Are all systems and networks that process intelligence data and/or information NSS?

A: Yes.

Question #13: Are all DoD systems NSS?

A: No, the exclusions in paragraph B of Title 44 quoted above precludes making all DoD systems NSS.

DATA SPILLS

Question #1: What is a data spill?

A: A data spill has been defined earlier in this FAQ as a security incident that results in the transfer of classified or sensitive (for example, privacy, contract sensitive) information to unaccredited and unauthorized information systems, applications or media. Data spills can be identified when either the originator or sender realizes his error, or when a reader discovers the spilled information.

The term data spill pertains to classified or sensitive information that is stored on or transmitted over information systems or networks that are:

- Not formally accredited to host or process that information (e.g., SCI to SIPRNET, Secret information to the NIPRNET.
- Not formally accredited to host or process information subject to specific restricted handling caveats (e.g., PROPIN, ORCON, NATO.
- Not formally accredited to host or process information under the control of a particular dissemination control system (e.g., HCS).
- The inappropriate release of information to a foreign nation's IS.

Question #2: What are the causes for data spillages?

A: Examples of data spillage causes include, but not limited to:

- Improperly handled media and media releases
- Improper data transfers
- Compilation of hidden, classified, or sensitive data in a file, in this sense, does not refer to data aggregation
    - Residual hidden data in a Word document
    - Embedded objects
    - Compressed files
    - Encrypted files
- User error
    - User fatigue
    - Lack of proper security training
    - Lack of trustworthy labels on data
- Contaminated data received from an outside source
- Data entry of classified information on an inappropriate system
- Process error
- Improper disposal

Question #3: Who is responsible for reporting a data spill, the sender or the recipient?

A: Both the sender and the recipient are responsible for reporting a data spill promptly when the disclosure incident is discovered. Depending on sensitivity and classification, information about the spill is entered into the databases at the Intelligence Community (IC) Incident Response Center (IRC), the DOD Joint Task Force-Global Network Operations (JTF-GNO), and the U.S. CERT. These organizations then coordinate about the spill response and reporting. The organization's data spill database permits identification of duplicate reports. Duplicate reports are highly preferable to failure to report a data spill.

Question #4: Can data, other than classified data, be "spilled?"

A: Yes, spilled data can involve compartments, handling or releasability controls, privacy data, proprietary data, personnel data, or any combination thereof.

Question #5: What is a privacy data spill?

A: A "privacy data spill" is the storage on, or transmission of, any information about an individual mentioned by the agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity (such as a person's name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual) over a system or network not approved for such information.

One of the primary objectives of the *Health Insurance Portability and Accountability Act* (HIPAA), was to protect a patient's Personally Identifiable Information (PII), as well as, establishing regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information about health status, provision of health care, or payment for health care that can be linked to an individual. The U.S. lawmakers are seeking ways to strictly limit the display, purchase, or sale of PII without the person's consent, as well as the prevention of acquiring PII through phishing[6]. U.S. lawmakers paid special attention to social security numbers because they could easily be used to commit identity theft. The *Social Security Number Protection Act of 2005* and *Identity Theft Prevention Act of 2005* each sought to limit the distribution of an individual's social security number.

The Office of Management and Budget (OMB) issued a Memorandum for Chief Information Officers (M-06-19) titled *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments Information*[7], 12 July 2006. This OMB Memorandum revises reporting procedures to include a requirement that all Federal agencies including the DoD and the Intelligence

[6] **phishing** is a form of criminal activity using social engineering techniques to attempt to fraudulently acquire sensitive information (e.g., passwords, credit card details) by masquerading as a trustworthy person or business in an electronic communication.

[7] **http://www.whitehouse.gov/omb/memoranda/ - Click on the "2006" link then click either M-06-15/M-06-16.**

Community shall report[8] all incidents involving PII[9] to the United States Computer Emergency Readiness Team (U.S.CERT) within one hour of discovering the incident. The procedures specify that all such reports should be in electronic or physical form, and the reporting agency should not distinguish between suspected and confirmed breaches. Further, the U.S. CERT must forward all agency reports to the appropriate Identity Theft Task Force point-of-contact within one hour of receiving the agency's notification.

Question #6: How do I report a data spill?

A: For SCI information, report the data spill to the network's information system security officer (ISSO), who should contact the agency's IRC, which will report the spill to the Director of National Intelligence's designated IRC.

Question #7: Should I delete the spilled data?

A: No! Do nothing other than to lock your system if you must leave it unattended, and immediately contact the organization's appropriately cleared ISSO.

Question #8: What does responding to data spill involve?

A: The following actions provide a "basic" framework for responding to a security incident.

1. **Assess**: Determine whether a data spill has actually occurred, the sensitivity of the information potentially compromised, and the number of users, systems and applications involved.
2. **Contain**: Identify all information hardware and software systems and applications affected, and execute approved procedures to ensure that the data spilled does not propagate further.
3. **Eradicate**: When authorized execute approved sanitization procedures using approved utilities to permanently remove the data spilled from contaminated information systems, applications, and media.
4. **Recovery**: Use a clean backup media, as-built documentation and approved procedures to recover and restore all affected information systems and applications to an accredited, secure configuration.

Question #9: How will the ISSO resolve a data spill?

A: The basic procedure for resolving a spill is documented in CNSS Policy No. 18, "*National Policy on Classified Information Spillage,*" June 2006.

[8] **http://www.us-cert.gov/federal/ - Incident Reporting Guidelines link is located under "Incident-Related Information"**

[9] Per OMB Memorandum: Personally Identifiable Information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Question #10: Why deal with data spills in a manner different from other security incidents?

A: The data that is spilled has an information owner. The information owner must be involved in the proposed remediation (e.g., ignore the spill, read recipients into a compartment or special access program, direct the erasure of the data) of the spilled data.

INCIDENTS

Question #1: Is a data spill a security incident?

A: Yes, but it is treated as a special type of incident, different from other types, and requiring different treatment, and consequently, reported and tracked through different systems.

Question #2: What makes a data spillage incident different from other kinds of security incidents?

A: All intelligence information has an information owner. In many cases, this is the DNI. In other cases, this is delegated to lower levels (e.g., Human Intelligence (HUMINT) data owned by the Director of Operations at the CIA). If data is spilled, the spill must be resolved in a manner acceptable to the information owner.

Question #3: Can these types of incidents or data spills occur only on classified or unclassified systems?

A: No. Historically, incidents have been introduced or transmitted between systems electronically or on media. These types of incident can occur on any system regardless of the different sensitivity or classification levels.

Question #4: Are there other types of security incidents beyond data spills?

A: Yes. In addition to data spills, some common types of security incident are:

- Root-level attacks on networking infrastructure, critical systems, or large, multipurpose or dedicated servers
- Compromise of privileged accounts on computer systems
- Denial of-service attacks on networking infrastructure and critical systems
- Compromise of individual user accounts or desktop (single-user) systems
- Scans of systems originating from the Internet
- Spam and mail forgery (e.g., phishing, pharming…)
- Viruses, worms and trojan horses
- Threats to individuals
- Co-mingling of law enforcement information with other classes of data

Question #5: What are some common indications that a security incident is occurring?

A: There are certain indications or "symptoms" of an incident that deserve attention, especially if they occur in combination with one another. These indications or “symptoms are:

- Unexplained system crashes preceded by anomalous system activity
- Bookmark or web site historical references that the user did not place on the system
- Inappropriate content on the system
- Login information not how the user left it
- High activity on an account that has had virtually no activity for months
- Many new files created without explanation, often with novel or strange file names

- Changes in file lengths or dates (e.g., a user should be suspicious if he/she observes that the .EXE files have grown)
- Data modification or deletion (e.g., files disappear or are corrupted)
- Denial of service
- Unexplained, poor system performance (e.g., unusually slow system response time)
- Indications of a virus (e.g., “I LOVE YOU” or "GOTCHA" message is displayed, or there are frequent unexplained system "beeps")
- Unexplainable log file entries (e.g., suspicious probes or browsing noted in the log files, numerous unsuccessful login attempts, the "sent" e-mail folder shows messages you did not send.)

None of the listed indications is absolute "proof" that an incident is occurring. There may be legitimate explanations for any of these symptoms. The important point to all computer users is to be aware of the symptoms and know how to react to them when suspicious activity is suspected.

Question #6: What are network attacks?

A: A network attack is a type of security incident intrusion, denial-of-service, or other attack on network infrastructure, computer system(s), or user account(s) conducted across a network. A network attack can be recognized by changes on the computer that were not made by the user, such as files erased or changed and programs running that the user didn't start. If a computer is operating much slower than usual, but only when plugged-in to the network, a denial of-service or other network attack may be in progress directed at the computer, the building, or the whole computer network. Rarely are network attacks directed at an individual person. More often, attackers are not intending to harm an individual; they are searching for an easily compromised computer from which to launch another attack.

Question #7: What are the objectives for efficient incident handling?

A: The objectives for efficient incident handling are:

- Ensure the integrity of critical systems and information
- Maintain and restore data as necessary
- Maintain and restore system service – minimize disruptions
- Identify the incident’s “modus operandi”
- Avoid escalation and further incidents
- Avoid unnecessary negative publicity
- Identify and help discipline the perpetrators

Question #8: Why report security incidents?

A: A security incident is a computer or network based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources. Security incidents may be observed, identified from audit files, or detected in real-time by detection software.

Security incidents should be reported to the organization because:

- A given security incident could be the first sign of a bigger problem; it is critical to promptly report it and to stop a potentially serious threat.
- It is clearly important to protect the confidentiality, availability, and integrity of classified or sensitive data. An incident can affect an organization's performance of mission-critical activities.
- There can be a public relations impact. News about security incidents tend to be damaging to an organization's reputation.
- If the incident is reported quickly less time is required to deal with the incident.

Question #9: I'll bet that I'm not the only one or even the first one affected by an incident. Why do I have to report it?

A: Reporting an incident may:

- Stop a potentially serious threat, if an incident is the first part or indicator of a larger problem.
- Reduce the time required to deal with that incident, especially if personnel are trained to handle an incident efficiently.
- Protect classified, unclassified sensitive, privacy, and proprietary information from further spillage, exploitation, or unauthorized disclosure.
- Prevent damage to an organization's stature among current or potential clients as news about computer security incidents tends to be viewed negatively.
- Avert the possibility of organizations or individuals being sued or criminally charged because one of their nodes was used to launch a network attack and they were either complicit or failed to exercise due diligence.

Question #10: What are the processes involved for resolving an incident?

A: Incident resolution relies on five interrelated processes to include:

- Protecting the information and information systems
- Reporting incidents via a step-by-step method
- Detecting attacks or intrusions
- Mitigating the effects of the incident and restore services
- Closing out the security incident by reporting and documenting lessons learned

COMMITTEE ON NATONAL SECURITY SYSTEMS

Question #1: What is the CNSS?

A: The CNSS was established under Executive Order 13231 of October 16, 2001, *Critical Infrastructure Protection in the Information Age, in which, the* President re-designated the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems.

The Department of Defense (DoD) chairs the CNSS under the authorities established by National Security Directive (NSD)-42. This was reaffirmed by Executive Order 13284, dated January 23, 2003, *Executive Order Amendment of Executive Orders and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*.

The CNSS provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems.

It should be noted that although the CNSS has purview over NSSs, all intelligence systems fall under the authority of the Director of National Intelligence (DNI). Nothing in this CNSS Issuance should be interpreted as altering or superseding the existing authorities of the DNI or the DNI's predecessor. In the event that any provision of this CNSS Issuance is inconsistent with guidance issued by the DNI, DNI guidance shall take precedence.

Question #2: What is the IDRRT?

A: The Investment in Detection, Response, and Recovery Technology (IDRRT) is a working group designated, established, and approved by the Subcommittee on Telecommunications Security and Subcommittee on Information Systems Security (STS/SISS) of the Committee on National Security Systems (CNSS). The IDRRT is charged to ensure minimum guidelines exist, and are made available, and can be applied in the detection of, ~~and~~ response to, and recovery from cyber incidents and intrusions through collaboration with existing government, private sector, and academia organizations.

Question #3: Are CNSS documents available on the Internet?

A: Yes, unclassified documents are available at the CNSS website - **http://www.cnss.gov/**

Question #4: How can I contact the CNSS?

A: Contact the CNSS Secretariat via:

- Electronic mailing address of - **cnss@radium.ncsc.mil**
- Office number - (410) 854-6805
- Secure Telephone Equipment (STE) – (410) 854-0217
- Unclassified Facsimile - (410) 854-6814

INTELLIGENCE COMMUNITY DEPARTMENT OF DEFENSE JOINT STAFF CONTACTS

Incident and data spill reports should go to the departments or agencies incident response team or equivalent. The agency's incident response team **-- *not the individual discovering the incident* --** *should make report to external organizations, based on the organization's incident response plan.*

Question #1: How can I contact the IC IRC?

A: Contact the IC IRC, 0530-1630, via:

- Electronic mailing address - **icircpmo@icirc.ic.gov**
- Office number - (301) 688-2059
- Secure Telephone Unit (STU) - (301) 688-2636
- Defense Secure Network (DSN) - (312) 644-2059
- Defense Red Switch Network (DRSN) - 228-2663
- NSA/CSS Secure Telephone System (NSTS)- 963-2021

Contact the NSA operations center outside of the designated hours via:

- Electronic mailing address - **nsocsiao@nsa.ic.gov**
- Office number – (301) 688-3495
- DSN - 312-644-3495
- DSRN - 228-2664
- NSTS - 963-4123

Question #2: How can I contact Joint Task Force-Global Network Operations (JTF-GNO)?

A: Contact the JTF-GNO via:

- NIPRNET (DoD CERT) website - **https://www.jtfgno.mil**
  The non-secure website was migrated to a secure PKI-enabled environment that requires a valid DoD certificate (e.g., DoD issued CAC, or other DoD issued PKI certificate) to access the new website location. Contact your local DoD security office if you need to obtain a DoD PKI Certificate.
- JTF-GNO J2 Intelligence Watch Officer
  Office number – (703) 601-6441
  DSN – (329) 6441
  Electronic mailing address - **intel_watch@jtfgno.smil.mil**
- SCI network
  NSTS - 461-5031
  Electronic mailing address **- Intel_watch@jtfgno.ic.gov**

Question #3: How can I contact the U.S. CERT?

A: Contact the U.S.CERT via:

- Unclassified website - **http://www.us-cert.gov/**
- Electronic mailing address - **soc@us-cert.gov**
- Secure website to report an incident - **https://forms.us-cert.gov/report/**