Security and Privacy Guidelines When Sharing Classified or Sensitive Data

Security and Privacy Guidelines when Sharing Classified or Sensitive Data

I. Overview

One of the key value propositions that the National Information Exchange Model (NIEM) provides is its ability to standardize a framework for information exchanges across domains. In order to provide a reasonable assurance of the confidentiality and integrity of the data being shared, it is imperative for NIEM to have guidelines detailing the best practices that NIEM members should follow to secure data. Similarly, it must be the responsibility of NIEM to provide a reasonable level of security assurance for participants to willingly provide their sensitive or classified information into the domain. This document describes the leading guidance of how classified or sensitive data is secured within an exchange.

"Sensitive" or "classified information" is information not otherwise categorized by statute or regulation that, if disclosed, could have an adverse impact on the welfare or privacy of individuals or the national interest. Examples of sensitive information include personal data such as Social Security numbers, trade secrets, system vulnerability information, etc.[1]

Securing sensitive or classified data within a domain requires a multi-layered approach. Ultimately, the security and privacy of the sensitive and classified data will be a function of the NIEM members' own information security standards. Thus, it is important that all NIEM members employ a minimum standard of information security protections to participate in the IEPD and information exchange process.

II. Industry Standards

It is the prerogative of each NIEM member organization to employ information security standards that are of adequate protection commensurate with the value of information stored. The guidelines of this document exist to demonstrate a portion of those standards, as well as to direct NIEM members as to where information about data security can be found.[2] At minimum, this approach consists of procedures for industry leading standards of security in the information, organizational and physical level.

A. **Information Security**

[1] With the exception of certain types of information protected by statute (e.g. Sensitive Security Information, Critical Infrastructure Information), there are no specific Federal criteria and no standard terminology for designating types of sensitive information. Such designations are left to the discretion of each individual Federal agency. "For Official Use Only" (FOUO) is the term used within DHS to identify unclassified information of a sensitive nature that is not otherwise categorized by statute or regulation.

[2] More information on the basics of information security standards can be found in DHS 4300A

A sufficient identity and access management program will also allow only authorized users with the appropriate credentials and required training to analyze information on the domain. Credentialed, role-based access management protections are crucial for information security and privacy considerations. Access review, along with an audit log and audit trail maintained by NIEM, will identify and limit the authorized user making a data request through a domain, the data of the inquiry, and the information that the authorized user has accessed. Additionally, a data retention program will allow information to be retained in a way so that it cannot be modified, accessed, destroyed or purged except by authorized domain users. Similarly, all sensitive and classified personally identifiable information (PII) traveling through the NIEM domain shall include, if possible, the name of the originating collector, the information system from which the information is provided, the date of collection, and the title and contact information for the data steward in the originating agency. All personally identifiable information with access restrictions will be marked when it is shared to reflect any limitations on access and sensitivity of disclosure.

B. **Organizational Security**

An organization's policy for protection of sensitive and classified data can only be as strong as the personnel's prerogative for implementation. Therefore, it is important that all personnel who utilize the NIEM domain exchange be aware of the necessity for information security and privacy. This includes an awareness of the consequences of non-compliance. Policies such as password guidelines, asset inventories, desk audits and regulation around use of real data in production can be helpful in implementing security and privacy by design in a NIEM member organization. Finally, training to employees and contractors on proper usage of the NIEM domains and information sharing is of paramount importance for any NIEM member organization. Security awareness training for all personnel in support of NIEM Exchanges should be mandatory, with additional targeted security training for personnel in special functions. It is important to have different levels of training based on users' familiarity with the concepts behind securing sensitive and classified data in the information space.

C. **Physical Security**

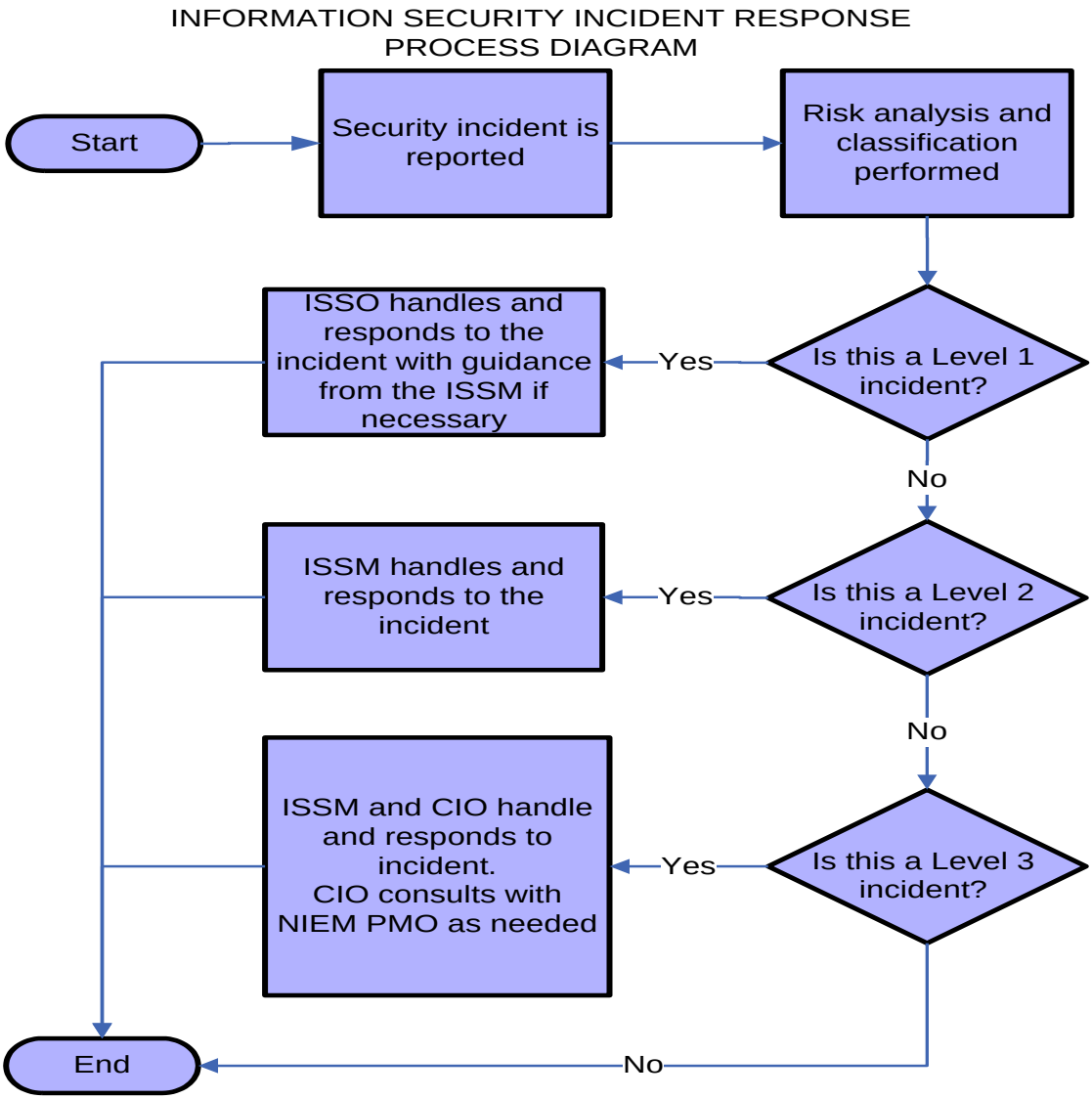
In order to best protect the security and privacy of sensitive or classified data, NIEM must have basic standards for physical security. This includes standards as to access to organization buildings, controls for detecting unauthorized access, and visitor procedures. Additionally, NIEM member organizations should have policies on secure workspaces including securing sensitive data in locked spaces at all times, encrypting flash drives, and preventing the downloading of sensitive information onto unauthorized media.

The guidelines established in this document contain these basic industry standards for the purpose of giving a reasonable level of assurance to NIEM members of the security standards of the exchanges and other organizations.

III. Incident Reporting

Before entering an information sharing partnership such as NIEM, members should have a procedure for how they will handle a security incident. Even with leading edge industry standards for protecting the privacy and integrity of shared data, security incidents can occur. Member organizations will find that during these incidents, it is very helpful to have an established repeatable protocol for action. One major part of this protocol is establishing, in advance, a categorization for security incident types. Without categorization, each incident must be handled in the same manner. That is neither practical nor efficient. Instead, having a security classification guide permits the organization to make quick data-driven decisions on action steps.

This figure shows a methodical way to review and respond to a security incident.



IV. Stakeholder Responsibilities

All NIEM stakeholders have a shared responsibility for assuring privacy information security. The table below displays some of the responsibilities of those within the NIEM community.

Stakeholder	Responsibilities
NIEM Community	Understand the procedures that NIEM takes to protect information in the domains.
NIEM PMO	Provide guidance on the protection of sensitive information in NIEM domains
NIEM NTAC	Review system architecture to ensure systems are adequately protecting data confidentiality and integrity.
NIEM ISSM	Provide assurance that the NIEM domain exchanges and NIEM members' information systems are at least as secure as required by NIST guidelines
Domain User	Document a request for the sharing of information through a NIEM domain that includes details on the rationale for the request and specific purpose as required by law.
Data Stewards	Limit the collection of sensitive data and consider implications of sharing information in NIEM domains.
Agency ISSO	Periodically review audit log to ensure that data is shared appropriately through the NIEM exchange
Functional Manager	Approve employee and contractor access to information systems. Periodically review employee and contractor access to sensitive information systems.

V. Tools & Resources

There exists a multitude of tools and resources available as members strive to protect sensitive and classified data in the domains. Many of these tools are considered industry standard and are being utilized by DHS and NIEM.

- Logging mechanisms such as Windows Event Log, firewall logs and Microsoft System Center Operations Manager, and standard Unix tools can audit system events for intrusions and specific uncharacteristic use.
- Industry leading Identity and Access Management protocols such as two layer authentication, Entrust tokens and Digital Certificates on USB tokens can provide additional security.
- Encryption Standards can utilize the VPN, IPSEC, Remote Desktop and Citrix protocols.

VI. References

- NIEM National Training Event (NTE)
- NIEM PMO and NIEM Committees
- NIEM training modules
- ISO 17799
- DHS 4300A
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987
- Public Law 107-296, Homeland Security Act of 2002
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources
- National Institute of Standards and Technology (NIST) Special Publications (e.g., 800-16, 800-34, 800-37, 800-50, 800-53) and Federal Information Processing Standards (FIPS) (e.g., FIPS 199, 200)