Controlling Security Sensitive Material (SSM)

May 31, 2017, 13:00 hrs EDT

Presented by: FERC-D2SI-Security

Agenda

- Objectives
- Terminology and concepts
- Security Sensitive Material (SSM)
- Threats
- Threat motivations
- Identifying SSM
- Marking and labeling
- Information Surety
- Establishing and conveying accountability
- Reducing threat exposure
- Reducing disruption impacts
- Mitigations measures to address elevated information surety risks
- Table of comparisons and examples
- Examples of mobile computing
- Templates and references
- Planning Considerations
- Next Steps

Objectives

- Guidance for a starting point for information security planning
  - Encourage better information security
  - Reduce confusion and disparity in the protection of SSM
- A tool for improving information security
  - Help identify what information is sensitive
  - Examples of how to manage SSM
- Not a prescriptive document
- Not intended to substitute as policy or set any minimum standard for compliance

Terminology and Concepts

- **Threat** – likely sources of harm
- **Threat Actor** – a willful threat
- **Security** – protection against threats
- **Access control** – selective restrictions
- **Security Sensitive Material (SSM)** – reveals information useful to attackers
- **Identifying SSM** – process of discovery
- **Responsibilities –** to identify SSM and establish risk-based protections and accountability
- **Markings and Labeling** – alert users of SSM
- **Authentication** – proof of validity
- **NDA –** non-disclosure agreement
- **Information Surety**
  - Limited Distribution
  - Timely Access
  - Reliable Content

Security Sensitive Material

- Common Security Sensitive Materials (SSM)
  - Site Security Plans
  - Vulnerability/Security Assessments
  - Internal Emergency Response/Rapid Recovery Plans
  - Cyber-security checklists
  - Cyber asset designation spreadsheets
  - Physical security checklists
  - References used to prepare such documents
- Nontraditional SSM sources
  - Work orders & inventory lists
  - HR records
  - Technical specifications
  - Network architecture and configuration settings

Threats

- Threats can stem from
  - Non-malicious sources activities, including: IT/mechanical system overhauls, database migrations, high personnel turnover, and business process disruptions
  - Compromised staff and external sources
- External threat actors do not have authorized access to non-public facilities or information
  - May trigger suspicion from wary non-threat insiders when seeking SSM
  - 5 of 13 Suspicious activities listed relate to SSM
- Internal threat actors have access to a licensee's/exemptee's SSM
  - May be unwittingly manipulated by external threats and circumstances or
  - May knowingly choose to carry out threat activities through action or passive inaction

Threat Motivations

Protection of SSM:

- To prevent misuse, malicious alteration, or destruction
  - Limited distribution/a need to know
  - Reasonable accessibility to authorized users during routine and atypical situations
  - Reliable content that is accurate and situation appropriate
- SSM represents an intellectual property investment

Threats seek SSM because:

- SSM, like the Site Security Plan, Vulnerability/Security assessment methodology, may also aid attacks against dams and/or critical assets

Identifying SSM

- Does the data and information contain details about critical assets, key facilities, systems, or vulnerabilities that would be useful for executing potential attacks?
- Does the information provide details about critical assets, key facilities, disaster recovery plans, incident response plans, and security configuration information?
- Does the information provide details about equipment layouts of critical cyber assets, similar diagrams, floor plans of computing centers that contain critical cyber assets, or network configurations?
- Would the information considered by itself or in conjunction with separate publicly available information be useful in developing and/or executing attacks on critical assets of a hydropower project or key facilities?

Marking and Labeling

- Clearly label SSM to identify its sensitive nature
  - bottom of each page/sheet, digital file, and/or folder
  - Include other SSM (e.g., display models and simulators

Privileged – Security Sensitive Material

“Do Not Release”

- The annual security compliance certification letter is the only SSM submitted by paper copy to FERC via USPS/FedEx/UPS
- SSM and CEII have security distinctions that are treated/handled differently
- Markings will not prevent deliberate information leaks

Information Surety

Involves a balanced protection strategy

- **Security** (limited access/distribution) – restrict the type, form, amount, and content of information available to appropriate personnel
- **Availability** (timely access) – ensure sufficient information is available routinely and in emergencies
- **Reliability** (trustworthy content) – ensure the information is accurate/appropriate in situations, error free or sneaky substitutions

Establishing and Conveying Accountability

- Disclosure Procedures and NDAs
  - Need to know
  - Tailored disclosures
- Rosters and Logs of SSM recipients
- Assigning ownership
- Policy training and acknowledgements
- Policy compliance measurements

Reducing Threat Exposure

- Staffing Precautions
- Physical Protections
  - Security
  - Minimization
  - Avoiding crib sheets
- Information Technology Protocols
- Managing Reproduction and Distribution
- Disposal/Destruction

Reducing Disruption Impacts

- Separate back-up files and working copies
- The back-up location can have more onerous access procedures
- Archives should be afforded at least equal, if not more stringent protections than primary data
- IT resilience ensures essential digital resources can withstand and/or quickly recover from common IT issues/failures
- Essential operating systems and digital SSM should have sufficient redundant capacity

Mitigation Measures to Address Elevated Information Surety Risks

- Use of two-person rule
- Memorization and training for urgent reflexive actions
- Pre-staging and pre-distilling SSM content for detailed information
- Tamper indicators and version controls,
  - Watermarks, version dates
  - Digital hashing
  - Challenge – response confirmations

Tables of Comparisons and Examples

- **Establish and convey accountability**
  - NDA disclosure practices
  - Rosters & Logs
  - Policies & Ownership
- **Reduce Threat Exposure**
  - Staffing Precautions
  - Physical Protections
  - IT Precautions
- **Network Precautions**
- **Mobile Computing**
- **Disposal/Destruction**
- **Reproduction and Distribution**
- **Reduce Disruption Impacts**
- **Mitigations for Elevated Information Surety Risks**
- **Enforcement and Policy**

Scenario examples of marginal, moderate and enhanced measures

Examples of Mobile Computing

Protection Scenario	Marginal Protection (examples)	*Also Add*	
		for Moderate Protection (examples)	*for* Enhanced Protection (examples)
Network protections	Using an internet service provider's internet protection program (e.g., MacAfee® or Norton™) and ensuring all operating system patches (e.g., Microsoft® Windows updates) are kept current	Using local networks created and maintained by a trained system administrator who keeps system patches, firewall settings, virus/malware protections current, and also monitors network logs for issues	Using networks that are locally administered by a well-resourced certified systems security professional (or CSSP), network firewalls with virus and malware protections, and internal filtering for key word [SSM] blocking

Templates and References

- DHS Examples
  - An Interagency Security Committee Guide: https://www.dhs.gov/publication/isc-resource-management-guide
  - DHS Management Directive 11042.1 and 11056.1 for Safeguarding Sensitive But Unclassified
  - DHS Management Directive: TSA's Best practices for non-government (contractor and sub-contractor) handling of government security sensitive information (SSI) is described at: https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf
- DOE directive for information security (DOE ORDER 471.6, Approved: 6-20-2011)
- NIST References
  - NISTIR 7621, Revision 1, Small Business Information Security
  - NIST Special Publications in the NIST SP-800-xxx series, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: https://www.nist.gov/publications/protecting-controlled-unclassified-information-nonfederal-systems-and-organizations

Planning Considerations

- Considerations before implementation
  - Human nature in routines
  - Limits of effectiveness
  - Precautions for accessing, producing, processing, sharing, handling, storing, transmitting, distributing, replicating, and destroying, regardless of media or format.
- Business culture tailoring
  - Paper vs. digital
  - Small team vs. distributed settings
- Information surety should not become a single point of failure for a site where an External threat with SSM can cause a catastrophic event

Next Steps

- Review period
  - Comments Due: June **16**, 2017
  - Submit suggestions to D2SI_HQ@ferc.gov
  - Final Draft of Best Practices for Controlling SSM, being posted today

- Editing and Distribution
  - Completed and ready to use by: June **30**, 2017

- Implementation
  - Non-prescriptive guide for use by Licensees/Exemptees


DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

Questions?