BEST PRACTICES FOR CONTROLLING SECURITY SENSITIVE MATERIAL

(Final Draft)

Federal Energy Regulatory Commission
Office of Energy Projects
Division of Dam Safety and Inspections

June 2017

TABLE OF CONTENTS

ACRONYMS

CEII	Critical Energy Infrastructure Information
D2SI	Division of Dam Safety and Inspections
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
Email	electronic mail
FERC	Federal Energy Regulatory Commission
GSA	General Services Administration
IT	Information Technology
NDA	non-disclosure agreement
NIST	National Institute of Standards and Technology
SSM	security sensitive material

DEFINITIONS

Access control—The selective restriction of entering or using a place or other resource.

Authentication (two factor)—The process or action of proving or showing something to be true, genuine, or valid. Two-factor authentication uses two independent means for proving or showing validity.

Crib Sheet—A concise set of unofficial notes used for quick reference.

Critical Energy Infrastructure Information (or CEII)—Engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: 1) relates details about the production, generation, transportation, transmission, or distribution of energy; 2) could be useful to a person in planning an attack on critical infrastructure; 3) is exempt from mandatory disclosure under the Freedom of Information Act, and 4) does not simply give the general location of the critical infrastructure (18 C.F.R. 388.113).

Degaussing—The process of decreasing or eliminating a remnant magnetic field (named after the gauss, a unit of magnetism, which in turn was named after Carl Friedrich Gauss).

Exemptee—An entity that owns a hydroelectric project that is not subject to the requirements of Part I of the Federal Power Act. The exempted project is, however, subject to mandatory terms and conditions set by federal and state fish and wildlife agencies and by the Federal Energy Regulatory Commission. Obtaining an exemption can be a more simplified process than an application for a license. Exemptions are issued in perpetuity.

DEFINITIONS

(continued)

Hard Copy—A printed or hand-written copy of a document.

Handling—The manipulation of information or data, including, but not limited to: creation, labelling (marking), electronic transmission (emailing, faxing, scanning, or sending by mail), hardcopy transmission (mail or courier), storage (electronic or hard copy), archiving, and reproduction (printing).

Licensee—An entity that holds the license for a hydropower project and is regulated by the requirements of Part I of the Federal Power Act.

Privileged—Manufacturers' proprietary or business confidential design information and cultural resource reports. Privileged documents are generally exempt from release pursuant to an act of Congress. Also, material that a submitter can justify as exempt from public release pursuant to Freedom of Information Act, Exemption 4. To qualify for Exemption 4 protection, the information must be: 1) commercial or financial, 2) obtained from a person, and 3) privileged or confidential. Generally, to be "confidential" for purposes of Exemption 4, disclosure of the information must either impair the government's ability to obtain similar information in the future, or cause substantial harm to the competitive position of the submitter of the information.

Security—Procedures followed or measures taken to ensure protection against a threat.

Threat—A person or thing that is likely to cause damage, danger, or other hostile action. Threats may be intentional, inadvertent, unwitting or circumstantial.

Threat Actor—A person who willfully takes deliberate action or inaction with the intent to cause harm.

Security sensitive material (or SSM)—Information that by itself or in conjunction with separate publicly available information could be useful in developing and/or executing malicious physical or cyber-attacks.

SUMMARY OF CHANGES

This Final Draft document is the latest revision to *Best Practices for Controlling Security Sensitive Material* since it was last revised on May 19, 2017. All changes made were based on the feedback from initial reviewers and discussions with industry experts. The following table contains a brief discussion of several changes in the guide (minor editorial changes are not identified here):

Page	Section	Description of Revision "Final Draft" Changes
All		Final draft with working group contributions

1.0 INTRODCUTION

The Federal Energy Regulatory Commission's (FERC) Division of Dam Safety and Inspections (D2SI) develops and implements policies, programs, and standards for dam safety, public safety, and hydropower security at and around projects that FERC regulates. D2SI is responsible for monitoring and auditing the security programs and measures that licensees implement at their hydropower projects.

Security sensitive documents are compiled during the responsible management of a hydropower project. Security plans are kept onsite either in a hard copy (printed or handwritten) form or secured digital form or stored offsite at corporate offices. Site operators prepare these documents to demonstrate to FERC how site staff will predictably deter, detect, assess, delay, respond, mitigate, and recover from potential plausible, credible security threats. Security plans, as well as the security assessment methodology used to generate these plans, contain information that could potentially be used to plan an attack against a dam and/or its critical assets. Therefore, the information used to prepare and compile security plans and vulnerability assessments should be treated as sensitive and should only be accessible and provided to users who demonstrate a legitimate need to know.

This document is intended to serve as a best practices overview for properly handling security sensitive material (SSM). It provides FERC and licensees/exemptees and their staff with examples and explanations about the secure handling and storage of security sensitive documents and common information about security practices. In this guidance, the term *licensee* refers to both licensees and exemptees.

2.0 OBJECTIVES

Licensees should always protect documents containing SSM that could be used for malicious acts. This protection should include limiting distribution and access to those with a legitimate need to know, making information reasonably accessible to authorized users for both routine and atypical situations, and ensuring the content is accurate and situation appropriate. Licensees and their employees should take proactive measures to protect SSM to ensure the continued safe and secure operation of their hydropower projects. Therefore, objectives of this guidance are to:

1. raise the awareness of a licensee about the importance of securing sensitive information;
2. provide information so that a licensee can better identify what information is sensitive and how to manage it; and
3. provide best practices on how licensees can protect SSM from external and internal threats.

3.0 SECURITY SENSITIVE MATERIAL AND THREATS

SSM reveals information, which by itself or in conjunction with separate publicly available information, could be used to develop and/or execute malicious physical attacks or cyberattacks. Site-generated SSM is valuable not only to licensees of hydropower projects but also to potential threat actors. SSM contains information that is not normally publically observable or available and that has been compiled and/or organized in a way that could be advantageous to threat actors. Licensees should be inherently interested in protecting SSM from being misused, maliciously altered, or destroyed. SSM is commonly associated with security plans, emergency response plans, and similar materials. SSM can be derived from normal business documents that, at first glance, do not appear to contain information that could be useful to threat actors.

3.1 Common Security Sensitive Materials

Common SSM includes those materials typically used by emergency responders and associated with site security and hazard mitigation. SSM is readily available in numerous documents, such as the methodology and references used to prepare site-specific security plans, vulnerability assessments, internal emergency response plans, cyber-asset checklists, physical security checklists, emergency response plans, and rapid recovery plans.

3.2 Nontraditional Security Sensitive Materials

Because threat actors can obtain SSM needed to plan attacks by obtaining information other than common site SSM and emergency response documentation, licensees should protect all SSM sources to ensure the continued safe and secure operation of their hydropower projects. Some easily overlooked information sources include documents that are rarely, if ever, used to complete the FERC-required security plans, including:

- Documented pre-hire screening procedures;
- Human resources files containing sensitive or embarrassing information that might be used to identify behaviors for social engineering or extortion;
- Detailed statements-of-work for contractors who service critical systems or produce critical designs, resources, or parts;
- Product/equipment specifications revealing interdependency links and interfaces between mechanical and digital operational equipment, and for vendor-published specifications, lists of in-service products, as appropriate;
- Compiled order forms, delivery schedules, accounts receivable/payable, billing and supply chain documents for critical components or parts that are assembled into or co-located with critical components;

- Authorization and verification protocols for equipment/work orders and deliveries; and
- Network architecture, including network settings, router settings, log-in/password settings, software versions (including firewalls), software patching protocols, programming recovery/re-start protocols, detailed network cabling diagrams, and data back-up and archival controls.

3.3 Threats

Licensees must protect themselves from both external and internal threat actors. External threat actors do not have authorized access to non-public facilities or information, while internal threat actors do have access to a licensee's SSM. Internal threats may be unwittingly manipulated by external threats and circumstances or may knowingly carry out threat activities through action or passive inaction. Internal risks to information surety can stem from compromised staff and non-malicious sources and activities, including IT/mechanical system overhauls, database migrations, high personnel turnover, and business process disruptions such as those endured during corporate takeovers and buyouts. External threat actors' attempts to gain SSM information may trigger suspicion from wary non-threat insiders.

The guidelines for suspicious activity reporting for threat assessments and counterterrorism list specific information to identify potential threat actors. Threat actors need information about their potential targets, so they can predictably plan and execute attacks that extend beyond impromptu attacks of chance or opportunity. Of the 13 categories of suspicious activities listed in FERC's Security Program for Hydropower Projects, the following 5 categories are related to SSM:

1. *Eliciting Information for an Unlawful Purpose*—Suspicious questioning of personnel by any means about particular structures, functions, personnel, or procedures at the facility or infrastructure;
2. *Recruiting*—Building operations teams and contacts, personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to personnel, facilities, or forces in transit;
3. *Surveillance*—Monitoring the activity of licensees, personnel, facilities, processes, or systems and showing an unusual interest (e.g., by observing through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or making video recording of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to personnel or facilities;

4. *Testing of Security*—Interacting with or posing challenges to facilities, personnel, or systems that could reveal physical, personnel, or cyber security capabilities, including attempts to compromise or disrupt information technology infrastructure; and
5. *Theft, Loss, and/or Diversion*—Experiencing theft or loss associated with a facility or infrastructure (e.g., badges, uniforms, identification cards, emergency vehicles, copper wire, technology, or documents, whether classified or unclassified) that are proprietary to the facility and/or diverting attention from a facility or infrastructure that is related to a theft or loss associated with that facility.

3.4 Responsibilities

Licensees should choose and implement the appropriate means, methods, and effective protections for their SSM (both hard copy and digital) based on the risks they face. In doing so, licensees are responsible for:

- Assessing the effectiveness of document control procedures to manage those risks;
- Securing SSM for projects during routine operations, security upgrades, and emergencies;
- Training appropriate staff on the selected document control procedures and ensuring that licensee and site staff adhere to the selected procedures as appropriate; and
- Ensuring that the staff holding and/or creating the SSM are appropriately classifying and labeling documents.

4.0 SECURE HANDLING OF SECURITY SENSITIVE MATERIAL

4.1 Identifying Security Sensitive Material

Licensees can potentially identify SSM by considering the following questions.

- Do 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?

4.2 Marking and Labeling Security Sensitive Information

Licensees and their employees are encouraged to clearly label all SSM to identify the sensitive nature of these materials. This process entails clearly labeling documents and data files (normally at the bottom of each page/sheet, file, and/or folder) and other SSM (e.g., display models and simulators). Such labels may include descriptions of appropriate distribution and warnings about misuse and/or inappropriate disclosure.

These markings serve to raise the awareness of authorized personnel during the appropriate, routine handling of information. Such markings also will alert unauthorized people that the information is sensitive and should not be further distributed or that site security officials should be alerted to a potential information leak. These markings will not prevent deliberate information leaks, and in some situations, they may highlight valuable information.

FERC requests that licensees limit submittals of SSM made to the agency to only their annual security compliance certification letters. Labeling SSM as: "Privileged – Security Sensitive Material" with "Do Not Release" on the next line is preferred for SSM provided to FERC, as shown below:

Privileged – Security Sensitive Material
Do Not Release

The use of bright lettering helps draw a reader's eye to this designation. Adopting the practice of marking every SSM page's headers and footer, including those not submitted to FERC, will reduce the potential for inadvertent disclosure and raise awareness of the sensitive nature of the information. Cover pages with similar markings may also be used on top of documents to further alert people to the need to protect the information and to shield the title pages from casual view.

SSM, which is privileged information, is different than Critical Energy Infrastructure Information, or CEII, because the public can request a copy of CEII through Freedom of Information Act requests after signing a nondisclosure form, while privileged information is protected through the FAST Act.

4.3 Information Surety

Information surety involves security (limited access/distribution), availability (timely access), and reliability (trustworthy content) into a balanced protection strategy.

4.3.1 Limited Distribution

Restricting the type of information that is available to staff and limiting its distribution to appropriate key personnel with approved access requires licensees to thoughtfully assess each unique site, user, and operating scenario. Achieving appropriate limits of distribution can greatly reduce the ability of threat actors from obtaining SSM. Limiting distribution involves controlling both the actual documents containing SSM and the detailed knowledge of their contents, to the greatest extent practicable, while safely and securely operating a dam. For example, a licensee may allow designated representatives of other organizations and oversight agencies (e.g., FERC inspectors) to review a security plan for a hydropower project because they have a definite purpose for needing to know this information; however, the licensee should never distribute hard copies or digital files of proprietary SSM to any outside agency or non-owner.

Limited distribution entails restricting the type, form, amount, and certain content of information that is made available to appropriate key personnel. For example, planning executives may need a general perspective on project operations, but they do not need specific information such as individual passwords and firewall settings. All personnel—whether security technicians, armed security personnel and law enforcement officers, equipment operators, or maintenance staff—have their own level of appropriate SSM access. For example, maintenance technicians may need to refer to blueprints of the powerhouse, armed security responders/law enforcement officers may need only a quick reference card to supplement training and drills, but senior operators may need to study procedures and emergency response plans each day to fulfill their job responsibilities.

4.3.2 Timely Access

In order for information to be valuable, it must be reasonably available in a timely manner and serve its intended purpose during both routine and atypical (emergency) scenarios. The concept of timely access balances limited distribution with the needs of authorized users, ensuring that sufficient information is available routinely and in emergencies.

Cumbersome or time-consuming decryption and/or document retrieval processes can delay response time during emergencies. Storing documents at distant locations or on computer networks that are left vulnerable to power surges and interruptions, internet viruses and malware, or denial of service attacks also may prevent project personnel from accessing data in a timely fashion. For example, if a technician or operator needs a

manual from a location that is inaccessible during flash floods or brush fires, the distribution is not limited, it is denied.

When developing policies about information surety, licensees should consider timely access because onerous distribution controls may prompt project personnel to develop unmanaged processes, or workarounds, to complete tasks. These unmanaged processes can present opportunities both for unauthorized disclosure of SSM and for the interjection (deliberate and accidental) of erroneous information.

4.3.3 Reliable Content

Content reliability requires that licensees ensure the information about their project is accurate and appropriate for the situation. Several forms of espionage involve information tampering or substituting outdated procedures into routine practices. At sites where espionage is a low risk, version control issues and outdated manuals may likely be the cause of erroneous content. For example, if critical equipment has been modified and operators and technicians are using outdated reference guides or informal crib sheets, instead of updated procedures, they may take inappropriate action. The application of appropriate quality control procedures for SSM ensures source materials are correct (free from errors or sneaky substitutions) and current. Establishing and enforcing policies to ensure that manuals and databases are version controlled, changes are logged (recording when and by whom), computers are protected against viruses and malware, and users of SSM only refer to version controlled reference materials (not crib sheets) will substantially support information surety.

5.0 PROCEDURES FOR MANAGING SECURITY SENSITIVE MATERIAL

This section presents information about procedures that are common in government facilities that handle security sensitive information. These procedures might be appropriately adapted to unique site conditions. Some of these procedures help assign accountability, create records for future use if/when a security investigation or audit is needed, reduce targets of opportunity, and reduce the potential disruption from information surety shortcomings. Other procedures address routine handling and measures for elevated information risk environments. The procedures alone do not provide for assessment or response, but they can aid licensees in deterring threats, initial alerting of threats, recovering from threats or attacks, and mitigating consequences.

5.1 Establishing and Conveying Accountability

When licensees establish and follow disclosure procedures, they can ensure that any person receiving SSM has a legitimate need to know the information, is authorized to receive the specific SSM, and understands their responsibility for protecting the SSM. Disclosure procedures help ensure that the SSM being disclosed is in the appropriate form and contains the appropriate level of SSM. These procedures often include non-

disclosure agreements (NDAs), which establish a hard copy record of who has received SSM and can greatly reduce future disputes about responsibilities for supporting company information surety practices; disclosure rosters, which identify personnel having access to SSM; visitor logs; audits; and assigned ownership.

NDAs provide written notification of a recipient's responsibility to protect information and specify the information to be protected. Regulators have an inherent duty to protect SSM within their legal limits. Licensees should consider having non-regulatory recipients of sensitive information sign NDAs. For example, a person requesting information from an information holder must clearly state what information is needed and in what format (e.g., a briefing, a data file, or a graph), the information holder then records the request description (including a brief description of content, format, and take away versus onsite review), and finally the information requester and the providing party sign the NDA.

Disclosure rosters are also beneficial to licensees because they provide a list of personnel with direct, unaccompanied access to source information, including who has received specialized training containing SSM. Disclosure rosters are particularly valuable during version control updates and in the event of a potential unauthorized disclosure. Licensees can review the roster when quality checking version controls or to narrow down potential sources of suspected information leaks.

Visitor logs provide records of who and when outsider visitors are granted access to secure spaces with controlled access. Such logs, like General Services Administration (GSA) Form 139 https://www.gsa.gov/portal/forms/download/114022), can be helpful in establishing an "escorted visitor only zone" and provide a formal record of visitors who have been granted access.

Policy compliance surveys and audits are essential to enforcing polices and assessing their impact. Audits and surveys confirm and reinforce only the behaviors that are being measured in the manner that the measurement is being taken. When designing an audit or survey, it is important to consider what is not being validated and if the criteria needs to be revised to avoid being misled by a correct answer to a wrong question. It is also important to use audits to encourage and reinforce a security mindset, rather than allowing personnel to create workarounds or crib sheets or engage in other undesirable behavior. In the absence of measuring (via surveys and audits), the security practices might be changed, but it is not possible to know whether information surety itself has been improved.

Assigned ownership for each document or set of SSM places a responsible person in charge of properly handling and protecting that information during normal operations, storage, (authorized) disclosure, disposal, and other business processes. Effectively

establishing assigned ownership requires listing sensitive information owners and users and periodically reviewing the lists to validate and verify that policies are being followed.

5.2 Reducing Threat Exposure

Licensees should take measures to reduce threat exposure by addressing perceptions that their SSM is vulnerable and preventing their SSM from being easily compromised (i.e., stolen, destroyed, or altered). Reducing both the perceived and real exposure of SSM to threats can be accomplished in many ways, as discussed below.

5.2.1 Staffing Precautions

Conducting pre-hire screening of both internal staff and outside contractors helps licensees reduce internal threats and also expose external threats actors attempting to gain access. Pre-hire screening methods and standards are driven by local labor laws and risk level justifications. Consulting local human resource specialists and legal counsel may likely be appropriate before implementing changes to current practices.

5.2.2 Physical Protections

Providing tailored excerpts of SSM for use by staff in specific operational roles (e.g., security forces versus mechanical technicians) prevents unneeded SSM risk exposure and also provides each user group with information that is specifically required for their informational needs. This user group-specific information can be secured in a pre-positioned location for people to access while operating away from their workstations, reducing the temptation to create crib sheets. For example, if a technician's work truck is secured during off-hours, then only the SSM the technician commonly uses while making repairs in the field might be kept locked in a tool compartment in the work truck, while the rest of his/her relevancy-tailored SSM remains secured at the central equipment repair facility. Or similarly, hints to remember special access codes used by security officials might be engraved on ammunition magazines that the security officials carry while they are on duty away from the security control room, but the special access codes would be locked in an armory or vault when the security officials are off duty.

If licensees or their staff are in possession of SSM when in publically accessible areas or while in transit, they should consider obscuring or wrapping SSM to hide the content (and value) of the materials as being targets of opportunity. Overt markings on the exterior of easily accessed/viewed documents may draw the attention of threat actors. Other precautions personnel should consider while traveling and attending offsite meetings with SSM include:

- Taking only the minimum, essential SSM needed for the event;
- When in transit, not leaving SSM in unlocked vehicles;

- Storing laptops and documents out of sight in locked compartments;
- Not leaving SSM unattended on a conference table; and
- Using the safe in hotel rooms to secure laptops and personal electronic devices containing SSM if leaving them in the room.

SSM should be stored in a secure container or location, such as a locked desk, file cabinet, or space where access can be controlled, after work hours and when otherwise not in use. Bolting down containers that secure SSM and using cable-locks on unattended laptops will prevent an unprepared thief from easily stealing a container or laptop in hopes of finding valuable information.

Changing locks and combinations at normal periodic intervals and whenever either a key is lost or a staff member with the combination leaves employment can greatly help reduce unauthorized access potential. Keys and combinations include mechanical keys, dial combinations, and electronic encrypting keys. The issuance and recovery of keys and combinations can be tracked on using a log such as GSA Form 138, https://www.gsa.gov/portal/forms/download/114010, to help support procedures for ensuing key locks and combinations are changed as needed. Some security lockers/safes are equipped with dual locks, each keyed differently, for situations where the risk assessment warrants requiring two people to open a locker or safe. Some secure digital file systems include features that provide separate user roles for requesting changes and authorizing changes to archived data and/or even for viewing protected files.

Safe and vault procedures include logging who and when a repository is accessed and confirming that the safe or vault was locked the night before. Logs, such as government Standard Form 702, https://www.gsa.gov/portal/forms/download/115582, narrow the time frame for confirming or eliminating concerns about suspected unauthorized access if a container is found open or damaged.

5.2.3 Information Technology Protocols

Implementing Information Technology (IT) protocols for electronic mail (email) accounts for site/company businesses allows site security and IT professionals to maintain the digital settings to better protect SSM. Mixing personal email with business email is not advised because it can lead to accidental data leaks, information ownership disputes, and other issues complicating information surety.

Timing out of screen locks with password protected screen savers ensures that computer screens do not leave the SSM viewable for extended periods and also greatly reduces the potential of an unattended computer or mobile device from being used to retrieve SSM data and files.

Encrypting hard drives for fixed and portable devices at the root command greatly reduces the exposure potential from lost and/or stolen computers. Encryption sophistication that exceeds the plausible credible threats for a particular site is generally considered sufficient. Procedures and policies that enforce using company/site-managed mobile devices (rather than personal devices) for processing SSM allows site security and IT professionals to maintain the digital settings to protect SSM.

Digital files and folders should be password protected to restrict viewing and/or printing of SSM to authorized personnel in possession of the passwords. Note: Password-protected Microsoft® Office documents do not meet most common encryption requirements for sending information externally.

Electronic files containing SSM should be stored on secured networks, servers, or computers with document management systems and file servers that are housed in facilities/rooms with controlled access.

5.2.4 Information Technology Filtering

Digital files and email headers can also be marked or labeled to identify the need to protect certain files. For example, a file might be saved as: "[SSM] Site SA, Update 2017.doc" and a sensitive email subject line may say: "[SSM] Site SA Updates." Network administrators can also append each outgoing (externally directed) emails with language declaring the proper use of email received, such as:

> All email to/from this account is subject to formal review and is for protected use only. Action may be taken in response to any inappropriate use of the (*Company Name's*) e-mail system. This email may contain information that is privileged, security sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of (*Company Name's*). If you have received this email in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

If file names and email subject lines include a standard marking, such as "[SSM]," a network administrator can scan and filter externally bound IT traffic to prevent or delay such content from being sent without proper authorization. Although inside threat actors can deliberately circumvent IT filtering, the use of a standard marking or label can be highly effective in preventing staff from inadvertently sending SSM.

5.2.5 Disposal/Destruction

Ensuring that discarded SSM is not later recovered by threat actors reduces unauthorized exposure from materials that are no longer being managed and protected. Precautions that may be taken during the disposal of SSM include the following:

- Material containing sensitive information should be discarded using secured shredding receptacles or other secured document destruction methods.
- Hard copies of documents should be destroyed by shredding or burning.
- Information on computer storage media should be destroyed by overwriting the media with random data, degaussing the media with a strong magnetic field, or fully destroying the media (e.g., disintegrating, pulverizing, melting, incinerating, or shredding).

5.3 Managing Reproduction and Distribution of Security Sensitive Material

Licensees should minimize copying and/or excerpting SSM and should follow these precautions:

- Reproduced SSM should be marked and protected in the same manner as the original work.
- Copies should be immediately retrieved from the copier/scanner and not left unattended.
- If the copier/scanner is not part of a secured internal network or located within a secure space where SSM is stored, its memory should be cleared (when technically feasible) to prevent additional copies from being made later using the copier's memory files.
- SSM should not be faxed as a means of distribution.

Licensees should transmit SSM to external networks or facilities only after taking appropriate precautions, which can include all or a combination of the following:

- Hard copies should be sent only by U.S. Postal Service first class, express, certified, or registered mail or a bonded courier.
- Digital items, which must be encrypted or password protected (e.g., WinZip, AES option with password), can be sent electronically using encrypted email, file share, or virtual private network or VPN). Corresponding passwords should be sent in a different, unassociated message and format, such as by phone or in an unrelated email that does not mention the document name or file that the password opens.

- Microsoft® Office password protection does not meet most common encryption requirements for sending information externally because it can be too easily defeated.

5.4 Reducing Disruption Impacts

Back-up files and documents should be separated so that the loss of one information repository (building or IT network) does not result in the complete loss of valuable information and should be stored separately in a different safe place, such as a secure escrow repository, hidden vault, corporate office, or elsewhere. The back-up location can have more onerous access procedures if it is intended to be accessed only in the event that the primary documents are lost or suspected of being tampered with or altered. Archives should be afforded at least equal, if not more stringent, protections to primary data in the event they are seldom checked. Encrypting archives is a simple way to help ensure that archived data remains secure from unauthorized disclosure.

IT resilience describes the concept of ensuring that essential digital resources can readily withstand and/or quickly recover from common issues such as internet service outages, individual hard drive failures, denial of service attacks, power disruptions/surges, and other IT issues. Ideally, essential operating systems and digital SSM should have sufficient redundant network capacity; firewalls or air-gapping; and co-located uninterruptable power supplies to ensure that a primary network or data center failure does not impede effective access to and implementation of security plans and emergency response plans.

5.5 Mitigation Measures to Address Elevated Information Surety Risks

Licensees can implement three important mitigation measures—limiting distribution, ensuring timely access, and ensuring the reliable content of SSM—to address the risks posed by lapses of information surety, suspected active external threats, or internal risk concerns. More stringent and less commonly used measures are easily implemented when circumstances warrant.

Limited distribution can be enforced through the separation of authority to access or amend the information containing SSM. In high-security government applications, the two-man rule is often applied. Under the two-man rule, “all access and actions require the presence of two authorized people at all times” (https://en.wikipedia.org/wiki/Two-man_rule). Two-man rule can be tailored to be as simple as providing one person the entry codes for the office alarm system and another with the keys to the filing cabinet. Implementing this simple rule would not prevent a threat, such as forced entry during an emergency, but it would prevent someone from casually gaining access without leaving obvious indications.

Timely access to key pieces of information that must be readily available can be ensured by having staff memorize content and providing staff with extensive training that includes drills and repetition. In some instances, especially emergencies, personnel cannot rely on reference manuals and correct interpretations of encrypted information. For example, the tactics, techniques, and procedures of security or law enforcement responders engaged in neutralizing armed attackers should be reflexive. Operational effectiveness normally warrants having all key operational staff commit all of their commonly used SSM to memory. Although staff should not be expected to memorize all SSM, implementing or using critical SSM should never be delayed because staff need to review manuals. (Note: Memorization of complex and intricate data without timely access to corroborating manuals can pose risks to information reliability, particularly as procedures or codes evolve.)

The reliability of content can be more greatly ensured when risk levels warrant more elaborate methods such as those employed to reduce financial counterfeiting. For example: 1) hard copies can be date limited, watermarked, embossed, or have other special printing features/paper to inhibit easy substitution of individual pages or whole sections; and 2) digital files can be logged with hash-values and version controls to readily reveal when files have been altered or substituted. Many other methods are available to ensure document security. The Document Security Alliance, a government and industry partnership organization dedicated to the practice of document security (www.documentsecurityalliance.com) has published papers and holds regular meetings in Washington, DC, to advance the subject.

6.0 PROTECTION COMPARISONS

While beginning with basic protection measures is far better than having no protection measures in place, licensees should strive to improve their SSM security measures as opportunities arise. As security efforts and discipline increase, a protection program matures. The following table provides examples of how security can mature with additional resources.

Protection Scenario	Marginal Protection (examples)	*Also Add*	
		***for* Moderate Protection (examples)**	***for* Enhanced Protection (examples)**
Identification of SSM	Unilaterally designating what material should be protected	Consulting stakeholders on discussions of what constitutes SSM and where it might be found	Researching guides, reviewing internal documents, and consulting with security professionals
Pre-screening employees	Verifying references, credentials, and resume experience	Running a credit and criminal records check	Completing a background investigation
Back-up storage	Storing a second copy in a different room or on a different computer network	Storing a second copy in a different building	Storing an encrypted, version-controlled copy securely offsite
Access control	Having locked cabinets and doors	Implementing key controls and combination changes on hardened containers	Implementing two-man-rule protocols for critical assets
Markings	Labeling documents (hard copy and digital) as SSM on all pages	Using cover pages with handling instructions and policy references	Using SSM file and folder designations sufficient for IT filtering
Limiting distribution	Only sharing or transmitting SSM to those with a verified need to know and using a protected method	Using NDAs for those without a stronger, legal obligation to protect the SSM	Obtaining transmittal receipts and tracking them to ensure later revision controls or disposal needs are met

Protection Scenario	Marginal Protection (examples)	*Also Add*	
		***for* Moderate Protection (examples)**	***for* Enhanced Protection (examples)**
Mobile computing	BYOD (bringing your own device) with separate log-ins for site accounts	Using separate devices for site work with strong password protections	Using devices and cyber security protocols, including encrypted hard drives and two-factor authentication, that are configured by the organization's IT security professionals, as opposed to Verizon, ATT, or individual users
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

Protection Scenario	Marginal Protection (examples)	*Also Add*	
		***for* Moderate Protection (examples)**	***for* Enhanced Protection (examples)**
IT resilience	Separating data back-ups and primary systems on uninterruptable power supplies sufficient for orderly shut-down	Having redundant power sources and internal redundant network resources (switches, routers, and processors)	Having multiple redundant servers, networks, and routers enabled in a real-time fail-lover configuration plus duplicate external connectivity to outside counterparts via fiber/cable, wireless, and satellite
Accessibility	Providing a digital master on the computers of key staff and hard copies in emergency response centers	Providing each user group with a working copy that is available (and properly secured) in the primary work location	Providing tailored SSM excerpts for each user group pre-positioned and secured where they will be needed
Reliability	Ensuring version controls with separate digital files and hard copies	Ensuring all reference materials are current through quality controlled, updated distribution and inspections	Placing tamper indicators on all distributed copies
Policy	Providing an informal, unsigned draft for each operational group	Established a fully developed security policy signed by the board of executives	Distributing signed policy to and briefing authorized SSM users
Training	Conducting new hire orientation	Conducting annual briefings	Requiring authorized users to complete an annual course and test

Protection Scenario	Marginal Protection (examples)	*Also Add*	
		***for* Moderate Protection (examples)**	***for* Enhanced Protection (examples)**
Enforcement	Casual monitoring	Completing compliance checklists	Conducting periodic structured audits
Security validation	Completing peer review and analysis of plans	Conducting table top exercises with key staff and stakeholders	Conducting practical exercises with role players for threats, bystanders, responders, and stakeholders

This document is intended to assist licensees to develop measures to the effectively protect SSM at their individual sites based on their assessed risks. The operating environment and potential future shifts are important considerations when assessing how best to adapt different information surety options. Some factors that may be used to determine what measures are appropriate for individual sites include whether the usual operating environment is:

- *Hard copy versus digital files*—If a site tends to operate with hard copy manuals and guides at work stations, the methods for document control likely revolve around manual processes such as sign-out sheets, management supervision, and process quality measures like those required for ISO 9000 certification. If workstations and manuals are largely digital, many of those functions can be supported and audited by a network system administrator.
- *Small functional team in a closed setting versus a large functional team in a distributed setting*—If a site tends to operate as a tight-knit group of co-workers, leadership that instills a sense of responsibility for SSM and mutual accountability is likely become to the driving factor because peer relationships become second to policy. If the operational environment functions as a distributed collection of resources without consistent peer groups, procedural discipline is likely to become the driving factor. It is important to consider the organizational culture when selecting an information surety strategy because the culture will help enforce (or erode) the desired security habits.

7.0 EXAMPLES AND REFERENCES

Having examples of information surety policies can assist licensees in establishing or adapting some or all of the procedures described in the preceding sections to create policies best suited for their project or site. Although licensees may find developing such policies easier if they have another organization's policy documents, appropriate practices and policies for handing SSM should be unique to each licensee and their individual sites. This section provides some examples that can be found online and is intended to stimulate ideas and encourage licensees and their staff to create policies that are suited to meet their individual needs.

7.1 Department of Homeland Security and Department of Energy Examples

The U.S. Department of Homeland Security's (DHS) best practices and sources include the *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide*, available at: https://www.dhs.gov/publication/isc-resource-management-guide. The Interagency Security Committee's *Policies, Standards, and Best Practices* along with other topics are available at: https://www.dhs.gov/isc-policies-standards-best-practices.

Other examples of how DHS and the U.S. Department of Energy (DOE) have developed policies for handling sensitive, but unclassified, information are available online, as noted below:

- DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, available at: https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf
- DHS Management Directive 11056.1, *Sensitive Security Information (SSI)*, available at: https://www.dhs.gov/sites/default/files/publications/DHS%20MD%2011056.1%20Sensitive%20Security%20Information%20%28SSI%29.pdf
- Transportation Security Administration's *Sensitive Security Information: Best Practices Guide for Non-DHS Employees and Contractors*, available at: https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf
- DOE Order 471.6, *Information Security*, available at: https://www.directives.doe.gov/directives-documents/400-series/0471.6-BOrder/@@images/file

7.2 National Institute of Standards and Technology References

The National Institute of Standards and Technology (NIST) has published multiple guides about information security and how to implement access control for government facilities, including:

- NISTIR 7621, Revision 1, *Small Business Information Security: The Fundamentals*, available at: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- Special Publication 800-160, S*ystems Security Engineering; Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
- *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, which provides federal agencies with a set of recommended security requirements for protecting the confidentiality of Controlled Unclassified Information in nonfederal systems and organizations, available at: https://www.nist.gov/publications/protecting-controlled-unclassified-information-nonfederal-systems-and-organizations
- Several other relevant NIST Special Publications also available in the NIST SP-800-xxx series

8.0 FINAL CONSIDERATIONS

All sensitive information should be protected by taking special precautions for accessing, producing, processing, sharing, handling, storing, transmitting, distributing, replicating, and destroying, regardless of media or format. Marking or labeling documents or files, IT filtering, and implementing the other practices discussed above cannot prevent the careless or deliberate mishandling of sensitive information. Licensees must ensure that the intended functions of site security procedures, Supervisory Control and Data Acquisition systems, emergency response plans, critical components, and others cannot be easily made to work against a site's safety and reliability through just the loss of information. If IT and physical infrastructure can readily be made to fail catastrophically by external threats in possession of unauthorized SSM, licensees should consider implementing additional mitigation measures so that a lapse of information security practices does not become a single point of failure for the site.