Security Guideline for the Electricity Sector: Protecting Sensitive Information

Preamble:
It is in the public interest for NERC to develop guidelines that are useful for improving the reliability of the Bulk Power System (BPS). Guidelines provide suggested guidance on a particular topic for use by BPS users, owners, and operators according to each entity’s facts and circumstances and do not provide binding norms, establish mandatory reliability standards, or create parameters by which compliance to standards is monitored or enforced.

Introduction:
This guideline addresses potential risks that can apply to some electricity sector organizations and provides practices that can help mitigate risks. Each organization determines the risks and impacts and the practices it deems appropriate to manage those risks.

Purpose:
It is recommended that all electricity sector infrastructure owners and operators\(^1\) have an information security or confidentiality policy in place as an integral part of their business-level policies.

Where applicable, the policy should address securing the production, processing, storage, transmission, and disposal of both physical and electronic data and information regardless of media type (paper, disk, hard drive, USB drives, etc.). The policy should define the hierarchical classification of Sensitive Information, as well as the authorization requirements and conditions for permitted disclosure.

Electricity sector owners and operators are encouraged to consider this guideline when deciding whether information should be made available to government agencies, third parties, or to the public in general. This guideline provides advice to electricity sector management, security and compliance personnel responsible for handling sensitive information. Also, this information is made available to the extent necessary for operational reliability. The dissemination of sensitive information should be given only to authorities and trusted partners with a legitimate need-to-know.

\(^1\) This guidance is presented to develop a general program. Some Responsible Entities are required under NERC Reliability Standards to have specific training and awareness programs that may go above and beyond what is recommended here.
Scope of Application:
This guideline applies to all electricity sector personnel as it relates to making information available to others within their organization as well as those outside the company or agency and those who handle sensitive information given to them from other companies or government agencies.

Guideline Statement:
Electricity sector entities expressed concerns that sensitive information regarding electricity assets could be used by those intending to damage critical facilities, disrupt electric operations or harm individuals. This has compelled electricity sector entities and government agencies to closely examine their policies and practices regarding the release of certain information to outside parties. The intent of this guideline is to provide background on five key areas of Sensitive Information:

- Identification of Sensitive Information
- Classification of Sensitive Information
- Labeling of Sensitive Information
- Security of Sensitive Information
- Sharing of Sensitive Information

Guideline Details:

Definition of Sensitive Information
Information can appear in many forms, including company reports, brochures and other promotional materials, Internet web sites, on-line documents, automated or personally conveyed information, and public records. Each company has proprietary information which it deems to be sensitive in nature and requires some level of protection from inappropriate or inadvertent disclosure.

In this Guideline, the term ‘Sensitive Information’ refers to any data or information that could be used by those intending to target electricity sector critical infrastructure, damage facilities, disrupt operations, or harm individuals. The term Critical Infrastructure Information (CII) includes information from all 18 sectors classified as Critical Infrastructure and Key Resources (CI/KR) within the United States, and 10 critical infrastructure sectors within Canada.

Identification of Sensitive Information
As a business process, it is important that electricity sector entities evaluate and identify information as sensitive as it relates to the production, processing, storage, transmission, and disposal, as well as the

---

2 The Department of Homeland Security has identified 18 critical infrastructure sectors, as diverse as food and agriculture, emergency services, transportation and information technology: http://www.dhs.gov/files/programs/critical.shtm
4 See Tables 1 and 2 for examples of potentially sensitive information
conditions for permitted disclosure, of that information. The following questions will help identify potentially Sensitive Information.

- As it relates to your company's critical assets, key facilities, or systems, does the information contain operational procedures, lists relating to critical assets and identified critical cyber assets, network topology or similar diagrams, floor plans of computing centers that contain critical cyber assets, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information?
- What impact on critical assets, key facilities, and the bulk electric system could the information have if it inadvertently reached an unintended audience, or was used in conjunction with publicly available information?
- Does the information contain personal details of key operating personnel such as biographical data, contact information, names, addresses, telephone numbers, etc?
- Could someone intent on causing harm to personnel or critical assets, key facilities, and systems use the information to his or her advantage?

**Classification of Information**

Once the decision is made to classify information, a further classification process may be required which will assist in the handling and processing of requests for information. This guideline offers the following suggested classifications:

- Public
- Company
- Restricted

**Public**

Data or information lawfully, properly and regularly disclosed generally or broadly to the public requiring no restrictions in producing, processing, handling, storing, transmitting, distributing, replicating or destroying information. Disclosure will not adversely impact the BPS or critical infrastructure. (For example, the physical location of a critical asset without any designation of criticality i.e., address of the company building housing a transmission control center.)

**Company (i.e. Internal Use, Private)**

Data or information regarding critical assets, key facilities, and systems maintaining the reliability and security of the BPS may require protective measures in its access, production, processing, sharing, handling, storage, transmission, distribution, replication or destruction of information. Inadvertent or unauthorized disclosure or modification could adversely impact the BPS or critical infrastructure. (For example, documents that are the property of the company and not to be further shared without permission i.e., one-line diagrams showing critical facilities.)

**Restricted (i.e. Confidential, Secret)**

Company data or information regarding critical assets, key facilities, and systems maintaining the reliability and security of the BPS may require secure restrictions in its access, production, processing,
sharing, handling, storage, transmission and distribution, replication, and destruction procedures and is typically not shared with other entities. Inadvertent or unauthorized disclosure or modification could severely impact the Company, BPS or critical infrastructure. (For example, results of engineering studies showing system weakness or vulnerabilities within the electrical system.)

**Labeling Non-Public Information**

It is the responsibility of the owner of the information to appropriately classify and label Sensitive Information.

If a person is handling a document which contains Sensitive Information and the document has not been properly designated, the document should be returned to the information owner for proper classification and designation.

This Guideline does not require specific labeling standards; however recommendations for labeling for Sensitive Information are below:

**Documents stored in an electronic format**

Below are samples of labels that might be appropriate. Each organization should determine labels suitable to its needs. It is recommended that the location and label wording be consistent throughout the document. A document watermark can also be used.

- **Sensitive Information - Company**
- **Sensitive Information - Restricted**

**Documents only available in hardcopy**

A hand stamp or other label can be used to provide markings equivalent to those listed above. It is recommended that the marking location be consistent on every page throughout the document, in particular for loose-leaf pages (e.g., ringed-binders, file-folders, etc.). A classification label on the cover and on the first page of the publication may also contain instructions to treat this documentation as a bound manual, and that removal of pages from this manual is prohibited, unless revisions are required. Hardcopies of bound documentation (permanent binding with no loose leafed pages) internal or from vendors can be stamped on the cover and on the first page of the publication. Consideration should be given to stating that the documents are the property of the Company and should not be shared without permission. One example of a Sensitive Information stamp is shown below:
All Sensitive Information requires additional precautions in accessing, producing, processing, sharing, handling, storing, transmitting, distributing, replicating or destroying, regardless of media. The information classification process determines the level of security. These guidelines may augment your organizations information classification and protection policy and procedures.

**Protection of Sensitive Information**
Entities are encouraged to utilize these guidelines in the development of their internal policies and procedures for protecting sensitive information.

**Controlling Access to Sensitive Information**
The program to manage access to Sensitive Information can utilize the current policies and procedures in place to control logical and physical access to information associated with critical assets and critical cyber assets. An annual review of user access to Sensitive Information should be considered. The following are some of the examples of what could be included in an annual review:

- Labeling
- Logical and physical storage
- Access rights
- Disposal
- Handling during transit (internal / external).

**Handling Sensitive Information Documents**
Company staff (full time, part time, temporary personnel and contractor/vendor) is responsible for safeguarding Sensitive Information in their custody or under their control. The extent of protection afforded Sensitive Information needs to be sufficient to reasonably prevent the possibility of its loss or compromise, inadvertent or unauthorized disclosure or modification.

It is recommended that the following precautions be taken when handling all Sensitive Information in any document, regardless of media, in whole or in part:

- **Protection** - Sensitive Information should be protected at all times by controlled access, appropriate secure storage or having it under the personal observation and control of a person.

---

5 Appropriate handling procedures for Sensitive Information should be followed whether within the confines of a secured company facility or in unsecured corporate/public facilities.
authorized to receive it. Each person who works with protected Sensitive Information is responsible for adhering to the established measures and precautions to ensure that unauthorized persons do not gain access to it.

- **While on corporate travel** be sure to physically secure laptops/personal electronic devices containing Sensitive Information
  - Consider locking up laptops/personal electronic devices in secure location
  - Consider using cable-locks when leaving a laptop unattended
  - Ensure your desktops and laptops conform to the company required desktop timeout and password security
  - Consider full hard drive encryption
  - Be aware of copiers that store electronic versions of copies. If possible, disable electronic storage on copiers used for reproducing Sensitive Information.

- **While working on drafts or revisions of Sensitive Information documents** be sure to secure working copies
  - Don't leave Sensitive Information documents laying available and unattended in unsecure areas
  - When in transit, secure Sensitive Information out of site or in a locked vehicle when possible
  - Store laptops and documents out of plain sight or in locked compartments when possible

- **Access to hardcopy Sensitive Information** - Controlling access to hardcopy Sensitive Information stored within facilities can be addressed appropriately within the company physical access control documentation. The document defines the administrators of those facilities where Sensitive Information is stored, the review processes and the process for removal of access for transfer, termination, and termination for cause.

- **Access to electronically stored Sensitive Information** - Controlling access to electronically stored Sensitive Information within the company provides a significant increase in the protection of that information. Topics to be considered in controlling such access include such things as:
  - Defining roles and responsibilities
  - Determining permissible storage locations for such information
  - Determining review processes and the removal of access for transfer, termination and termination for cause
  - Annual reviews and reports of the controlled access
  - Document management system access list reviews

- **Use and Storage** - Protective measures and precautions should be taken to minimize the risks of access to Sensitive Information by unauthorized personnel. Policies and procedures could
include references and/or links to the Incident Response procedure for monitoring and inappropriate release of information.

- **Physical Storage**
  - After working hours, facility security should not be the only method for protecting Sensitive Information. Sensitive Information should be protected in a secure container such as a locked desk or file cabinet.

- **Electronic Storage**
  - Unless otherwise mandated, it is recommended that Sensitive Information have an assigned owner.
  - Review owner and user lists to validate and verify.
  - Sensitive Information and non-Sensitive Information can be co-mingled in the folders/file structures and directories or database. It is important that personnel understand that the access security of the non-Sensitive Information and data inherits that of Sensitive Information.

- **Reproduction** - Documents or material containing Sensitive Information may be reproduced to the minimum extent necessary consistent with the need to carry out official duties provided that the reproduced material is marked and protected in the same manner as the original material.
  - It is recommended that Sensitive Information items be retrieved from the office equipment immediately.
  - When a Sensitive Information document is copied, scanned or printed, the document may be electronically stored on the local device and the recipient device. Wherever possible, all local and recipient copies should be deleted upon completion of task. Note: Sensitive Information normally should not be faxed.

- **Disposal** - Providing for secure destruction of Sensitive Information is crucial to any information protection program. Material containing Sensitive Information should be disposed through secured shredding receptacles or other secured document destruction methods.
  - Paper documents should be destroyed with a shredder or burned.
  - Information on computer storage media should be destroyed by one of the following methods:
    - Clear: Overwriting the media with random data
    - Purge: Degaussing the media with a strong magnetic field
    - Destroy: Methods include disintegration, pulverization, melting, incineration and shredding.

---

6 See Table 1 & Table 2
7 See Table 1 & Table 2
8 via means such as described in NIST SP800-88 Policy for Media Sanitization
- Unless already included, Companies may update record retention policy with instructions on handling Sensitive Information.

- **Transmission (Sending Externally)** - When sending *externally* outside the company, Sensitive Information can be transmitted by a secure method, such as corporate email, or by any of the methods suggested for external transmission, such as:
  - First Class mail with appropriate packaging and labeling;
  - E-mail with an encrypted file that is password protected and encrypted using an option such as AES.
    **Caution!** The password should not be included in e-mail. Deliver password using a separate means such as by phone or in an unrelated e-mail not mentioning the document name.
    **Note:** It is important that the encryption used is adequate. As general rule, encryption satisfying the requirements of US Federal Information Standard 140-2 or its successors is sufficient.
  - Secure file transfer protocol (SFTP) to external (Internet) sites or internal (intranet) sites can be sent using a password that is exchanged using a separate means.

- **Transmission (Sending Internally)** - When sending *internally* within the company, Sensitive Information can be transmitted by one of the following means:
  - E-mail subject line can note that Sensitive Information is contained within and the following disclaimer is recommended to be included in the body or at the end of the e-mail.
    **Disclaimer:**
    _The sensitivity of the information contained in this email has been classified under the Company Data Classification Program as Sensitive Information. The recipient of this information is required to follow the procedures outlined in the Company Data Classification Procedure._
  - Interoffice mail envelope should be appropriately labeled.
  - Secure file transfer protocol (SFTP) to external company sites or internal company sites can be sent using a password that is exchanged using a separate means.

**How to respond to requests for Sensitive Information**

In the course of business, companies will receive requests to deliver Sensitive Information to NERC, regulators, governmental agencies, and other authorities and utilities. It is important to have a robust internal procedure and protocol for handling Sensitive Information. It is equally important to be assured that Sensitive Information given to others will be handled with the same level of protection. Companies may consider designating a single person or department as being responsible for reviewing all third party requests for Sensitive Information, in particular reviewing information to be placed in the public domain. Where applicable, the designated person or department should collaborate with the company’s legal counsel on requests for Sensitive Information.
Releasing Sensitive Information Documents

Organizations are encouraged to develop an appropriate list of questions to be answered prior to releasing Sensitive Information to outside entities. Topics to be addressed may include, but are not limited to:

- Does the outside entity have a legitimate need for the information?
- Does the outside entity have a statutory, regulatory, or other right to the information?
- Will the outside entity provide adequate protection for the information?
- How should the organization notify the outside entity of the sensitivity of the information?
- Does the organization have external guidance that applies to such release?
- Does the outside entity understand appropriate disposal methods of the information?

If there is a legitimate business need-to-know, the sender may require the recipient of the Sensitive Information to complete a Non-Disclosure Agreement (NDA) and retain a copy on file in accordance to company retention policies. Sensitive Information should not be released unless there is a legitimate need-to-know.

In general, restriction of Sensitive Information may be necessary unless one of the following conditions is met:

- The entity requesting the data is specifically entitled to it pursuant to business needs, contractual obligations, regulatory or statutory requirements. Although compelled to provide the information, companies should ask that the recipient entity follow the minimum protections laid out in their sensitive information policy or appropriate laws for the handling of Sensitive Information.
- There is a trusted partner relationship and a NDA on file.
- It is required by a legislated mandate or legal requirement.

While entities often share Sensitive Information on a voluntary basis for the benefit of the electric industry as a whole, entities must maintain information security throughout this exchange process. The originator should notify the recipient of the need for protection of all Sensitive Information.

In certain situations entities will be requested to deliver Sensitive Information to NERC or a Regional Entity. Procedures are in place for NERC and the Regional Entities to exchange confidential information related to evaluations, audits, and investigations on condition they continue to maintain the confidentiality of such information.9

Protection of Sensitive Information shared with the United States Government

The Department of Homeland Security (DHS) has an information protection program to enhance information sharing between the private sector and the government, called the Protected Critical

---

9 For a full description of the NERC process for requesting and protecting information from Registered Entities, see section 1500 & 1600 of the NERC Rules of Procedure: http://www.nerc.com/page.php?cid=1|8|169). Please check with your Region for the most current procedures and/or direction.
Infrastructure Information (PCII)\textsuperscript{10} program. This program provides asset owners/managers with information security assurances when working with government partners. To take advantage of this program and those protections, Sensitive Information needs to meet certain standards.\textsuperscript{11} See Appendix A for more detail on the DHS PCII program.

**Protection of Information shared with the Canadian Government**

Canada’s Emergency Management Act (EMA) includes a consequential amendment to the Access to Information Act (ATIA) that allows the Government of Canada to protect specific critical infrastructure information supplied in confidence to the government by third parties. Canadian Critical Infrastructure (CI) owners and operators within the private sector should note that critical infrastructure information can be protected under this exemption only if it is appropriately marked and is treated as confidential by the entity that provides the information. It should also be noted that exemptions from disclosure for reasons of national security and public safety exist under federal/provincial/territorial access and freedom of information legislation. Canadian CI owners and operators (private sector) must appropriately classify and consistently protect CI information that is shared with the Canadian Government in order for it to be protected and exempted from release to a request under the ATIA.

**Protections of information shared with a 3\textsuperscript{rd} Party, Trusted Partner**

Third parties, such as energy companies, consultants working for such companies, developers, or others who can demonstrate a legitimate business need-to-know, may be provided information. It is recommended that third parties sign a nondisclosure agreement agreeing to protect Sensitive Information from misuse and to not distribute the information outside their control.

- **What is a Trusted Partner?**

  An exchange of information between entities, Regions, NERC or other utilities is considered “trusted” only if a set of prior agreements such as a Non-Disclosure Agreement (NDA) has been executed to document that trusted relationship. It should be assumed that unless an NDA is in place, any exchange between entities is accessible to the public and will not be held to the level of security assigned by the document’s originator.

  Is law enforcement a trusted partner? When it comes to handing over entity identified Sensitive Information, law enforcement is not entitled to this information unless it is pertinent to an ongoing criminal investigation, or it is given voluntarily by the entity to help with law enforcement activities. This statement does not imply that law enforcement cannot be a trusted partner. It means that the trusted partner relationship needs to be developed. Registered entities will, at some point, rely on the contacts made with law enforcement and these contacts may need to know specific information about entity facilities, such as security posture, emergency contacts, or hours of operations. With this information law enforcement will be

\textsuperscript{10} DHS covers 18 sectors within the PCII program and uses the term Critical Infrastructure Information (CII). [http://www.dhs.gov/files/programs/editorial_0404.shtm](http://www.dhs.gov/files/programs/editorial_0404.shtm)

better equipped to respond to emergencies or provide detailed threat analysis for critical facilities.

- **Freedom of Information Act (FOIA)**\(^{12}\)
  The FOIA law establishes a presumption that records in the possession of Executive Branch agencies and departments are available to the public. It is the vehicle under which the public may request Federal Government records in accordance with its requirements. Pursuant to the CII Act, PCII is exempt from disclosure under FOIA.

- **Sunshine Laws**
  Although investor owned utilities may handle 3rd party requests for information by developing a Confidentiality Agreement or Non-Disclosure Agreement (NDA), various governmentally owned entities do not have this luxury. These entities, which may include; federal, state, municipal, and some cooperatives are required to operate under what is termed “sunshine laws” which require public access to almost all documents used for daily operation of the business. Entities complying with federal, state and in some cases local ordinances while required to protect Sensitive Information can create a conflict. In most cases the entity dealing with the request will need to seek legal advice, but it is recommended that entities have a robust internal procedure for handling Sensitive Information.

- **Handling Sensitive Information from another Company or Agency**
  During the normal course of business or during an emergency situation, companies or agencies disclose or share information regarding critical infrastructure to maintain the availability and reliability of the BPS. Information originating from external sources should be handled with the same precautions and restrictions as defined in this guideline while augmenting an individual company’s internal policies and procedures. This information is entrusted to companies or agencies requiring precautions in its access, production, processing, sharing, handling, storage, transmission, distribution, replication or destruction. Those entrusted to handle Sensitive Information should know and understand any contractual, legal or regulatory requirements about the information provided by an external company or agency.

**Responding to Inadvertent or Unauthorized Disclosures of Sensitive Information**
It is recommended that companies have in place processes to respond to disclosures of Sensitive Information to ensure that they are addressed promptly and appropriately\(^{13}\). This process may include informing and involving senior management, market participants, government agencies, regulators, law enforcement, the public and the media, as appropriate.

Many states have laws regarding the response to an unauthorized release of sensitive personal information. One of the first and most modeled is California Security Breach Information Act (SB

---


This type of law defines the identification of Sensitive Information and the notification responsibilities of an entity in the event of a breach.

An unauthorized release of Sensitive Information poses a risk to the reliability of the BPS. This risk comes from a potential attacker gaining information as to the configuration and/or operation of the BPS, its control systems, or the security systems for the entity.

The potential for misuse of Sensitive Information resulting from an unauthorized disclosure is a primary concern. Depending on the information compromised, the entity should consider the potential misuse of the information and take steps to mitigate the potential threat vectors. Evaluation of the disclosure may require a team with cross-functional skillsets, dictated by the type of information. It is highly recommended that the mitigation efforts be documented as part of the incident response.

Communication is critical to the effective handling of an incident and response to an incident. An unauthorized disclosure of Sensitive Information could impact many areas of the organization. The impact may even extend outside the organization to neighboring entities, the region, or nationally. The impact of the disclosure on the reliability of the BPS should be evaluated during the incident response and communication plans included as part of the response.

A critique at the end of the event can be a useful method to reduce the possibility and impact of future events. The organization may not feel that every event needs a critique. If so, prudence would indicate that the organization provide guidance on when a critique is needed. The critique should involve personnel involved in the breach as well as the response and mitigation efforts. The deliverables from the critique can include:

- the root cause of the unauthorized disclosure,
- recommended actions to prevent a repeat event,
- review of the effectiveness of the mitigation efforts,
- review of the effectiveness of the response process,
- recommended improvements to controls,
- recommended and updated improvements to response process,
- recommended improvements for notification to the originator that the information was disclosed, and includes notification if the information was from another entity.

**Personnel Training on Handling Sensitive Information**

The electricity sector infrastructure owners and operators are encouraged to conduct training and ongoing employee, contractor, and vendor awareness sessions to ensure that information is appropriately secured. After the initial training, consider periodic reviews (every 12 or 24 months), as

---


15 This guidance is presented to develop a general program. Some Responsible Entities are required under NERC Reliability Standards to have specific training and awareness programs that may go above and beyond what is recommended here.
well as making information protection an integral part of your cyber security awareness program, providing personnel with reminders of their obligations and responsibilities.

The organization may consider training that includes:

- Clear explanation of the importance of protecting Sensitive Information and consequences of disclosure
- Clear definition of Sensitive Information
- Clear descriptions of the Sensitive Information classifications
- Clear descriptions of the protective measures and secure restrictions by classification
- Clear explanation on how these guidelines augment company policy and procedures
- Who to contact within the company for clarification and additional information
- How to respond to an unauthorized disclosure

Examples of Potentially Sensitive Information
The following table identifies generic categories of information that, if it became available to those intending to do harm, could place critical infrastructure at greater risk from terrorist or other criminal attacks. Critical infrastructure owners and operators are encouraged to use these categories to identify Sensitive Information relevant to their own security programs. The term “critical assets” includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BPS.
Table 1 - Examples of Potentially Sensitive Information by Information Type

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Locations &amp; Functions:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Critical assets: function and physical location | • Major generation facilities and associated switchyards  
• Black start facilities  
• Extra high voltage stations  
• Locations and responsibilities of control and operating entities  
• Details of critical computer systems (e.g. operational systems such as EMS, SCADA, digital control systems, network configuration and firewall schemes) |
| Network topology maps                      | • Ties between control areas, congestion points  
• GIS data of identified critical asset transmission networks and facilities, etc.  
• Hierarchical production or process control maps, charts or diagrams  
• Cyber assets and devices used for physical and electronic security |
| Exposed/unprotected assets                 |                                                                                                                                                                                                          |
| Unmanned assets                            | • SCADA-controlled assets  
• Remotely controlled assets |
| Hazardous materials                        | • Fuel, industrial chemicals or waste storage  
• Emergency coordination centers  
• Emergency meeting points and stations |
| Contingency facilities                     |                                                                                                                                                                                                          |
| Assessments:                               |                                                                                                                                                                                                          |
| Vulnerability or risk assessments          | • Security assessments (physical and electronic); Tiger-Team, Penetration Tests  
• Reports with findings, gap analyses, remediation or mitigating plans |
| Audits                                     | • Security audits (physical and electronic)  
• Reports with findings, gap analyses, remediation or mitigating plans |
| Hypothetical impact assessments            | • Hypothetical environmental impact assessments  
• Information that describes areas likely to be affected by a failure (e.g. downstream impact of dam breach, pump storage) |
<p>| Asset assessments                          | • CIP-related critical assets (CA) and critical cyber assets (CCA) lists, and associated lists and asset assessment documents |</p>
<table>
<thead>
<tr>
<th>Drills and exercises</th>
<th>Facility limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Detailed exercise scope and objectives</td>
<td></td>
</tr>
<tr>
<td>• Findings and lessons-learned</td>
<td></td>
</tr>
<tr>
<td>• Storm or other high-risk limits</td>
<td></td>
</tr>
<tr>
<td>• Grid constraints and congestion points</td>
<td></td>
</tr>
<tr>
<td>• Natural hazard high-risk facilities</td>
<td></td>
</tr>
<tr>
<td>• Single contingency risks</td>
<td></td>
</tr>
</tbody>
</table>

**Operations:**

<table>
<thead>
<tr>
<th>Real time operations data</th>
<th>Physical and cyber security plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Real time MW and flows at critical grid locations or transfer points</td>
<td></td>
</tr>
<tr>
<td>• Facility and information technology security capabilities and procedures</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security operating procedures</th>
<th>Heightened risk operating procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Firewall hardening configurations</td>
<td>• Critical production processes</td>
</tr>
<tr>
<td>• Server hardening configurations</td>
<td>• Contingency protection measures</td>
</tr>
<tr>
<td>• Incident detection system (IDS) or Incident prevention system (IPS) configuration</td>
<td>• Special protection schemes and their operation</td>
</tr>
<tr>
<td></td>
<td>• Emergency control actions, procedures and status when responding to events</td>
</tr>
<tr>
<td></td>
<td>• Details of response to NERC Alert Levels</td>
</tr>
</tbody>
</table>

**Emergency response and business continuity plans**

| • Emergency response procedures |
| • Facility evacuation criteria |
| • Power system restoration plans |
| • Contingency procedures |
| • Minutes of meetings regarding emergency planning processes and strategies |
| • Post-incident audits or reviews and specific action plans |

**Interdependencies:**

<table>
<thead>
<tr>
<th>Personnel information</th>
<th>Energy and water sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Critical operations or emergency personnel names, addresses, telephone numbers, contact information, etc.</td>
<td></td>
</tr>
<tr>
<td>Energy and water sources</td>
<td>Regular or backup energy and water sources</td>
</tr>
<tr>
<td>Communications assets and procedures</td>
<td>Critical communications processes and facilities</td>
</tr>
<tr>
<td>Transportation methods</td>
<td>Key communications contacts and protocols</td>
</tr>
<tr>
<td></td>
<td>Key transportation routes for critical services or personnel</td>
</tr>
</tbody>
</table>
### Key suppliers or customers

- Supply lines to critical facilities
- Critical key business process partners
- Customer supply points
- Number of retail customers served by a specific facility or portion of the Infrastructure
- Emergency and backup services
- Information that could be used to identify customers and their critical Infrastructure
<table>
<thead>
<tr>
<th>Table 2 - Examples of Sensitive Information[^16]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists identifying Bulk Electric System facilities as Critical Assets</td>
</tr>
<tr>
<td>Lists identifying specific cyber assets as Critical Cyber Assets</td>
</tr>
<tr>
<td>Operational procedures which specifically deal with:</td>
</tr>
<tr>
<td>- Access control</td>
</tr>
<tr>
<td>- Change control</td>
</tr>
<tr>
<td>- Configuration Management</td>
</tr>
<tr>
<td>Annual assessment of Critical Cyber Asset information protection program and action plan to remediate deficiencies</td>
</tr>
<tr>
<td>Configuration details of cyber devices associated with CIP program</td>
</tr>
<tr>
<td>Lists of personnel having logical or unescorted physical access to Critical Cyber Assets or electronic access control and monitoring or physical access control systems associated with Critical Cyber Assets</td>
</tr>
<tr>
<td>Network topology diagrams of Electronic Security Perimeters including devices interconnecting at electronic access points</td>
</tr>
<tr>
<td>Operational procedures specific to the configuration or management of the Electronic Security Perimeter including all associated Electronic Access Points or electronic access control and monitoring including:</td>
</tr>
<tr>
<td>- Firewall access control lists</td>
</tr>
<tr>
<td>- Ports and service listings</td>
</tr>
<tr>
<td>- Access control procedures</td>
</tr>
<tr>
<td>- Electronic access monitoring procedures</td>
</tr>
<tr>
<td>- Security monitoring correlation rules</td>
</tr>
<tr>
<td>Cyber vulnerability assessment results, action and mitigation plans</td>
</tr>
<tr>
<td>Operational procedures for securing dial-up access to Electronic Security Perimeters</td>
</tr>
<tr>
<td>Physical Security Plan</td>
</tr>
<tr>
<td>- Building diagrams identifying Critical Cyber Asset locations</td>
</tr>
<tr>
<td>- Measures to control entry at PSP access points</td>
</tr>
<tr>
<td>- Processes, tools, &amp; procedures to monitor physical access to the PSP</td>
</tr>
<tr>
<td>- Procedures for response to physical security incidents or alerts</td>
</tr>
<tr>
<td>- Procedures for control of special locks or keys associated with an ESP</td>
</tr>
<tr>
<td>Physical access logs of devices identified in the Physical Security Plan for protecting an ESP</td>
</tr>
<tr>
<td>Maintenance and testing procedures for the PSP</td>
</tr>
<tr>
<td>Physical Security survey results</td>
</tr>
</tbody>
</table>

[^16]: Registered entities with critical assets (CA) are recommended to validate minimum requirements for protecting sensitive information based on current NERC CIP Standards: [http://www.nerc.com/page.php?cid=2%7C20](http://www.nerc.com/page.php?cid=2%7C20)
<table>
<thead>
<tr>
<th>Documented test procedures and results associated with Cyber Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedures for patching Cyber Assets</td>
</tr>
<tr>
<td>Lists of software loaded on Cyber Assets</td>
</tr>
<tr>
<td>Documentation associated with anti-malware software on Cyber Assets</td>
</tr>
<tr>
<td>Process for updating anti-malware software on Cyber Assets</td>
</tr>
<tr>
<td>Procedures associated with account control for Cyber Assets</td>
</tr>
<tr>
<td>Lists of user and shared accounts for Cyber Assets</td>
</tr>
<tr>
<td>Logs associated with Cyber Assets</td>
</tr>
<tr>
<td>Documentation showing password policies for Cyber Assets</td>
</tr>
<tr>
<td>Documentation of security monitoring systems associated with Cyber Assets</td>
</tr>
<tr>
<td>Correlation and Alerting rules for security monitoring of Cyber Assets</td>
</tr>
<tr>
<td>Communication and escalation procedures associated with security monitoring of Cyber Assets</td>
</tr>
<tr>
<td>Log review procedures and records for Cyber Assets</td>
</tr>
<tr>
<td>Incident response plan for Cyber Assets</td>
</tr>
<tr>
<td>Incident Documentation and associated evidence for Cyber Assets</td>
</tr>
<tr>
<td>Documents associated with incident response testing, critiques, and remedial action plans</td>
</tr>
<tr>
<td>Recovery plan(s) for Cyber Assets</td>
</tr>
<tr>
<td>Disaster recovery exercise documentation including critiques and remedial action plans</td>
</tr>
<tr>
<td>Backup and storage procedures associated with Cyber Assets</td>
</tr>
<tr>
<td>Backup testing procedures and results for Cyber Assets</td>
</tr>
</tbody>
</table>
Definitions:
The following definitions apply in this guideline and may not be fully derived from the “NERC Glossary of Terms”.

**Access Control:** A process by which a system or individual makes decisions on access and rights to resources based upon established policy and the verified identity of an individual or other system.

**Authentication:** To positively verify the identity of a user, or other entity, often as a prerequisite to allowing access to resources.

**Authorization:** Granting a subject (individual, information system, process, application, etc.) access rights and associated privileges (read, write, modify, delete, etc.) to information and information systems.

**Critical Assets:** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. (Source: NERC Glossary of Terms)

**Critical Infrastructure (CI):** Systems and assets, whether physical or virtual, so vital to the United States or Canada that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

**Critical Infrastructure Information (CII):** Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems.

**Critical Energy Infrastructure Information (CEII):** (Source: US Federal Energy Regulatory Commission) CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical energy infrastructure (physical or virtual) that:

1. Relates details about the production, generation, transmission, or distribution of energy;
2. Could be useful to a person planning an attack on critical infrastructure;
3. Is exempt from mandatory disclosure under the Freedom of Information Act; and
4. Gives strategic information beyond the location of the critical infrastructure.

**Critical Cyber Assets:** Cyber Assets essential to the reliable operation of Critical Assets. (Source: NERC Glossary of Terms)

**Cyber Assets:** Programmable electronic devices and communication networks including hardware, software, and data. (Source: NERC Glossary of Terms)

**Need-to-know:** The determination made by an authorized user of information that a prospective recipient requires access to specific information to perform or assist in a lawful or authorized function, i.e. access is required for the performance of official duties.

**Protected Critical Infrastructure Information (PCII):** PCII refers to all critical infrastructure information, including categorical inclusion PCII, that has undergone the validation process and that the PCII Program Office has determined qualifies for protection under the US CII Act. (Source: US Department of Homeland Security)
**Vulnerability:** A flaw that provides for potential exploitation of information or information systems. This is not limited to flaws of a technical nature, but may include weaknesses in policies, standards, processes, and procedures, administrative controls, and physical location or layout.

**Vulnerability Assessment:** A systematic examination of an information system, database, or other application to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after the implementation.

**Revision History:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Version Number</th>
<th>Reason/ Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 14, 2002</td>
<td>1.0</td>
<td>Original</td>
</tr>
<tr>
<td>September 19, 2011</td>
<td>2.0</td>
<td>Update</td>
</tr>
<tr>
<td>October 19, 2011</td>
<td>2.1</td>
<td>CIPC review and comment</td>
</tr>
<tr>
<td>February 27, 2012</td>
<td>2.2</td>
<td>Update</td>
</tr>
<tr>
<td>March 2, 2012</td>
<td>2.3</td>
<td>Team review and update</td>
</tr>
<tr>
<td>March 9, 2012</td>
<td>2.5</td>
<td>Release to CIPC for approval to move to Industry Review</td>
</tr>
<tr>
<td>June 1, 2012</td>
<td>2.6</td>
<td>Team review and update</td>
</tr>
<tr>
<td>June 20, 2012</td>
<td>2.7</td>
<td>CIPC Approval</td>
</tr>
</tbody>
</table>
APPENDIX A
United States Government Protected Critical Infrastructure Information (PCII) Program

Protection of Sensitive Information shared with the United States Government

DHS has an information protection program to enhance information sharing between the private sector and the government, the Protected Critical Infrastructure Information (PCII) Program. It assists in building closer relationships with asset owners/managers, including those in the energy sector, by providing them with assurances that they can work with government partners without exposing their infrastructure information to disclosure. To take advantage of this program and those protections, information needs to meet certain standards.

First, it must meet the legal definition of CII, found in the Critical Infrastructure Information Act (CII Act):

“Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems, [consisting of] records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.”

Second, for that CII to be protected, it needs to be validated by the PCII Program Office at DHS. There are several different processes established for validation, depending on the needs of the submitter, and more information on the process can be found at the PCII Program website. Once information is protected as PCII, safeguarding measures and requirements ensure that precautions are taken to prevent unauthorized persons from overhearing conversations, observing PCII materials, or otherwise obtaining such information. PCII may be accessed only by

- Authorized and properly trained individuals,
- Who have homeland security responsibilities,

18 http://www.dhs.gov/pcii
• Who have a need to know the specific information, and
• Who sign a Non-Disclosure Agreement (if they are non-Federal employees).

There are penalties in place for the unauthorized release of PCII. Federal, State and local government employees who do not follow safeguarding procedures may be subject to disciplinary action including criminal and civil penalties and loss of employment. State laws governing theft, conspiracy and trade secrets may apply to government employees and contractors who intentionally mishandle PCII. DHS also works with various government partners to integrate PCII protections into their data-collection processes, ensuring that information is protected regardless of which government entity currently holds it.

Only government employees or contractors may access PCII. The critical infrastructure information (CII) that is retained by the submitter is not subject to the handling restrictions and limitations imposed by the CII Act and is not marked as PCII. It is worth noting that the definition of PCII overlaps somewhat with the definition of CEII which overlaps with the definition of Sensitive Information as described in this guideline. Therefore, information which qualifies as Sensitive Information may also qualify for the protections of PCII, but may still be shared between entities for operational purposes.

When CEII is submitted for protection and successfully validated, it becomes PCII. The CEII label would no longer apply to any copy of the information that has been validated as PCII. Potential submitters are, again, encouraged to consult the PCII Program website for more information (http://www.dhs.gov/pcii)