Personnel Security Clearance Task Force (PSCTF) Report

CIPC Approved on June 11, 2013
Table of Contents

Table of Contents ................................................................. 2
Executive Summary ............................................................... 3
Overview ............................................................................. 3
Task Force Objectives .......................................................... 3
Recommendations ............................................................... 3
Chapter 1 – Introduction ....................................................... 4
Task Force Focus ................................................................. 4
Limitations ........................................................................... 4
Overview of the NERC and PSCP Relationship ......................... 4
The Need for Clearances ....................................................... 5
Chapter 2 – Current State of Security Clearances ..................... 8
Overview ............................................................................. 8
Current Protocols for Granting Clearances ............................... 8
Clearance-Holding Organizations .......................................... 8
PSCP Process ...................................................................... 8
Applicant and Clearance Holder Requirements .......................... 9
Chapter 3 – Setting Expectations and Establishing Guidance ....... 10
Overview ............................................................................. 10
Develop Priority Guidance for Organizations ........................... 10
Designate the Appropriate Individuals .................................... 11
Know the Process .................................................................. 11
Gather Personal Data in Advance and Adhere to Deadlines .......... 11
Attend Briefings and Establish Contacts .................................. 12
Using Classified Information – Parallel Construction ................. 12
Register and Pass Clearances ................................................ 12
Chapter 4 – Clearance Model for Industry ............................... 14
Model Overview ................................................................... 14
Using the Model ................................................................... 14
Select Job Functions ............................................................. 14
Maximum Number of Clearances ........................................... 15
Chapter 5 – Findings and Recommendations .......................... 16
Findings .............................................................................. 16
Recommendations ............................................................... 16
Appendix I: Other Federal Departments and Agencies that Sponsor Clearances ......................................................... 18
Fusion Centers ..................................................................... 18
Federal Government Departments and Agencies ....................... 18
One-Day Read-Ins .................................................................. 18
Appendix II: Security Clearance Process .................................. 20
Executive Summary

Overview

Access to classified government threat and vulnerability information for certain electricity industry subject matter experts (SME) and executives is essential to support the reliability and operational security of the North American bulk power system (BPS). Both industry and the government recognize the importance of information sharing for situational awareness. Therefore, the two entities worked together to develop the classified information-sharing process from government-led, one-way briefings for a small number of cleared industry personnel to real-time collaboration between government and an increasing number of industry experts. To support Presidential Executive Order (EO) 13636 and Presidential Policy Directive (PPD) 21 (PPD-21), this highly valuable but limited program must be expanded to make more clearances available so that appropriate industry SMEs and executives may participate.

The North American Electric Reliability Corporation (NERC) Personnel Security Clearance Task Force (PSCTF) of the Critical Infrastructure Protection Committee (CIPC) offers guidance to help organizations identify, prioritize, and nominate the top four candidates at BPS organizations for U.S. government security clearances. This report also contains direction for those applying for clearance and for approved candidates seeking information on how to most effectively use their clearances.

The findings and recommendations presented in this report refer exclusively to the NERC CIPC process for obtaining security clearances through the U.S. Department of Homeland Security (DHS) Private Sector Clearance Program (PSCP) to enhance information sharing between the U.S. Government and owners and operators of the BPS.

These recommendations are not comprehensive regarding who should apply for security clearances. Specifically, this report does not address coordination among other critical infrastructure sectors and cross-sector interdependencies, which may identify additional clearance nominees outside those based on the NERC functional model. The proposed model—described in Chapter 4—may be adapted and used more broadly throughout the Energy Sector, and even across other sectors, as guidance for prioritizing clearance applications within an organization.

Task Force Objectives

The CIPC established the PSCTF to (1) review the government’s legal and policy requirements of industry for obtaining and maintaining security clearances; (2) examine protocols for granting private sector clearances; (3) develop recommendations for the CIPC and the Electricity Sub-sector Coordinating Council (ESCC) on the number and level of security clearances for the Electricity Sub-sector industry members; and (4) develop a clearance model that will aid industry in determining which Electricity Sub-sector personnel should be nominated for U.S. government security clearances.

Recommendations

The PSCTF’s key recommendations are:

1. Inform government of the value of that industry SMEs bring to classified discussions.
2. Use the clearance model outlined in this report to identify and validate industry nominees on a functional basis.
3. Submit clearance nominees through the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) to facilitate the selection process.
4. Encourage clearance nominees to use the guidance in this report during the PSCP application process.
5. Encourage clearance nominees to use this report’s guidance to meet their obligations as clearance holders.
6. Advocate that the ESCC requests additional Top Secret–Secured Compartmentalized Information (TS-SCI) clearances for ES-ISAC staff, as well as select SMEs with specific skill sets who will populate the ES-ISAC Hydra network.
7. The ESCC should recommend that the federal government reconcile the different personnel records systems by sector to increase clarity and ease efforts in passing clearances between departments and agencies.

---

1 For the purposes of this report, the PSCTF uses the term bulk power system (BPS). BPS is defined in section 215 of the FPA as (1) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (2) electric energy from generation facilities needed to maintain transmission system reliability. See 16 U.S.C. 824o (a) (1).
2 EO-13636 and PPD-21 are both dated February 12, 2013.
3 Hydra is an ES-ISAC-vetted volunteer reserve of experts selectively called on as needed to assist in rapidly developing threat mitigation strategies.
Chapter 1 – Introduction

Task Force Focus

The NERC CIPC and federal government departments and agencies have identified the need for additional industry SMEs and executives to obtain U.S. government security clearances to review classified materials related to threats to the industry. These reviews will (1) facilitate a more adequate determination of the potential impact to electric power systems and critical infrastructures based on improved subject matter expertise; (2) allow for recommendations for improved intelligence gathering; and (3) improve the government’s ability to provide more timely and actionable threat information to the entire Electricity Sub-sector. Having additional cleared personnel available to turn classified information into information that can be released at the For Official Use Only (FOUO) level will benefit industry as a whole and enable greater protection of critical infrastructures.

CIPC established the PSCTF to:

1. Review the U.S. government’s legal and policy requirements as applicable to industry personnel who obtain and maintain security clearances;
2. Examine protocols for granting private sector clearances;
3. Develop recommendations for CIPC and the ESCC on security clearances for industry members; and
4. Develop a model for industry to use in determining which personnel should seek a security clearance from the government.

The PSCTF analyzed DHS’s PSCP, the primary organization that sponsors clearances for private sector partners and administers the security clearance program for critical infrastructure protection (CIP).

While Secret-level clearances are available to larger audiences, the PSCTF believes that access to more Top Secret-level clearances would greatly enhance the information sharing dialogue between cleared industry and government personnel. Significantly more information is available at the TS-SCI level than is available at the Secret level. The small number of TS-SCI clearances currently available limits knowledgeable SME involvement in analysis and discussion of sensitive information and may slow or obstruct the identification of potential mitigation activities.

The PSCTF recognizes that programs and agreements that allow classified information sharing exist between the U.S. government and governments of other countries, such as Canada. However, the task force limited its focus so that this report addresses security clearances for U.S. citizens only. The Canadian Electricity Association has developed criteria to assign industry clearances in coordination with National Resources Canada.

Finally, the PSCTF recognizes that other CIPC task forces (i.e., Information Sharing and Security Metrics) are examining issues related to but outside the scope of this task force. Efforts emerging from those task forces may need to be reconciled with the PSCTF’s findings and recommendations in future CIPC guidelines.

Limitations

The PSCTF recognizes that federal government budget and staffing constraints may limit the number of clearance applications processed for the Electricity Sub-sector. With these restrictions and limitations in mind, the PSCTF suggests that each organization should follow the proposed model in this report to internally prioritize its nominees. Furthermore, each organization should engage in discussions with the ES-ISAC to facilitate submission of qualified nominees to the PSCP for U.S. government security clearances.

Overview of the NERC and PSCP Relationship

In 2003, Homeland Security Presidential Directive (HSPD) 7 presented the framework for information sharing between the federal government and private sector organizations that own critical infrastructure and key resources (CIKR). This

---


5 HSPD-7 has been superseded by PPD-21, “Critical Infrastructure Security and Resilience.” While these changes have occurred, the basic premise of the information sharing framework still exists, as established by HSPD-7. According to PPD-21, it “establishes national policy on critical infrastructure security and resilience” and “refines and clarifies the critical infrastructure-related functions, roles, and
framework included the development of Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC). NERC chairs the ESCC, which provides executive-level leadership and coordination for the Electricity Sub-sector of the Energy Sector within this framework.

The ES-ISAC and the ESCC provide a forum for the federal government to coordinate with industry on CIP matters. These authorities give each CIKR sector broad latitude to organize its SCC and Information Sharing and Analysis Center (ISAC) to address the needs of sector members.

Collaboration between the ESCC and the Energy GCC helped establish the current relationship between the PSCP and the CIPC. Originally, private sector representatives who obtained clearances through the PSCP fell under three disciplines of CIPC voting membership: Operations, Physical Security, and Cybersecurity. Representatives from the three major trade associations—American Public Power Association, the Edison Electric Institute, and the National Rural Electric Cooperative Association—were also invited to apply for clearances.

The PSCP is located within the DHS National Protection and Programs Directorate in the Office of Infrastructure Protection (IP). The PSCP sponsors security clearances for representatives from all 16 critical infrastructure sectors. These CIKR representatives are identified in the National Infrastructure Protection Plan partnership framework and are critical infrastructure owners and operators, sector leadership (e.g., SCC members), or SMEs that DHS identified to assist in analyzing critical infrastructure-related national security information.

The Need for Clearances

Access to classified government information by select industry SMEs and executives most familiar with—and most suited to respond to—industry threats would greatly increase security situational awareness within industry. Both industry and government recognize the importance of this information sharing. As a result, the classified information sharing process has transitioned from government-led, one-way briefings for a small number of cleared industry personnel to collaborations between expert government and industry personnel in the classified space. While this increased information sharing is a positive step, more individuals require clearances to help keep pace with the growth of these information exchanges. Industry experts are more familiar with the systems that operate the BPS and can best provide context for threats and vulnerabilities to the systems. This level of expertise does not usually reside with the government.

CIPC's work with its U.S. government partners requires robust, timely, reliable, and secure information exchange. The government provides security threat briefings to cleared sector representatives; these briefings may inform the products the CIPC task forces and working groups develop. Some of the briefings have led to industry alerts and modifications to NERC Reliability Standards (e.g., remote access and virtual private network vulnerabilities). In other instances, industry alerted the government to issues impacting the sector, which resulted in government-hosted classified briefings to inform a broader industry base. These exchanges have proven to be useful—occasionally critical—and should be expanded to include broader subject matter expertise.

The CIPC recognizes the value of operational context that subject matter expertise can provide for information that might otherwise be overlooked or undervalued by the Federal Intelligence Community (IC). In a recent report, the CIPC-led Cyber Attack Task Force offered the following recommendation:

---

6 Two U.S. authorities establish the federal framework for working with the U.S. private sector on infrastructure protection: Presidential Decision Directive 63 (PDD-63) and HSPD-7. PDD-63 encourages the formation of ISACs that would “possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility, and acceptability.” PDD-63 at p. 13–14, available at: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. HSPD-7 provides that DHS and sector-specific agencies “will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms . . . [and] shall collaborate with the private sector and continue to support sector-coordinating mechanisms: (a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and (b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.” HSPD-7 at p. 5–6; available at: http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

---
Continue to Extend Public/Private Partnership – More and more U.S. and Canadian electricity sector staff has been granted clearances to see classified information. As the U.S. and Canadian Intelligence Communities working with NERC discover new vulnerabilities and threats, this information should be disseminated to the electricity sector as quickly as possible. The electricity industry must ensure an appropriate mix of operational, security, technical, and managerial staff is cleared and available to evaluate, respond, and make timely decisions to slow or stop an attack.

Effective information sharing can be enabled in multiple ways including having clearances passed to local Federal Bureau of Investigation (FBI) offices and fusion centers so expedited secure communications can be accomplished with a wider portion of the industry. It is important to ensure the inclusion of the appropriate representation from the law enforcement community, as the traditional separation of tactical field operations and national security operations do not necessarily facilitate the proper sharing of information. In Canada, jurisdiction for Canadian electricity utilities varies from province to province. The provincial law enforcement agencies (LEA) have a reporting relationship with the Royal Canadian Mounted Police (RCMP).

In addition, NERC and federal agencies should continue to involve sector experts to help translate classified information (e.g., preparing useful tear-line material) into alerts that can be issued to the industry. This re-enforces the life cycle approach to addressing vulnerabilities.

The ES-ISAC offers an increasingly robust portal environment to organize electronic collaboration and this development effort should be strongly supported. ES-ISAC is establishing protective procedures to provide insulation from compliance concerns which might otherwise limit the willingness to share vital security information before, during or after a contingency. In the event standard information sharing protocols are unavailable during an attack (e.g. between utilities, ES-ISAC, etc), alternative methods need to be defined.

In parallel, the electricity sector needs to improve its sharing of information with federal agencies. Historically, there has been and continues to be a reluctance to do this because of the uncertainty about where the information could end up or that the disclosure could result in a perceived compliance violation.8

Given the significantly increased threat tempo and number of threat vectors posited against industry over the last 24 months, NERC CIPC recognizes the need for additional cleared industry SMEs and executives with increased access levels beyond that of the collateral Secret information historically provided. NERC and its registered entities benefit from additional clearances and improved information sharing, particularly since DHS established the National Cybersecurity and Communications Integration Center (NCCIC) in 2009. The NCCIC is a facility “where operational elements involved in cybersecurity and communications reliance are coordinated and integrated.”9 NCCIC partners include federal government departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities.10 The center’s activities provide greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions.11 Due to their specific skill sets and operational activities, ES-ISAC staff members are the NERC representatives best able to support NCCIC efforts; however, to engage in the public–private information sharing activities conducted on the NCCIC floor, ES-ISAC staff must have TS-SCI clearances.

Finally, executive personnel with understanding of industry needs can significantly contribute to the information sharing process. For example, intelligence analysts may have a limited understanding of the BPS and impacts on industry, which could prevent them from gathering and sharing pertinent information. Providing clearances to CEOs and other top industry executives allows for direct engagement between decision makers. It would also assist with the dissemination of information and appropriate allocation of limited industry resources. Supported by cleared SMEs, executive personnel will

---

8 LEA can be local police, sheriff, state police, FBI, or other agencies.
10 http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
11 Ibid.

contribute to a more thorough understanding of complex and rapidly changing issues, such as cyber threats, and give proper credence to risk management considerations within their organizations.

A recent National Infrastructure Advisory Council (NIAC) report supported the need for additional security clearances and called on the PSCP to “streamline the process for providing private sector security clearances . . . and develop opportunities for departing government personnel to keep or easily renew clearances when moving to key security positions in critical infrastructure companies.”\(^\text{12}\) The importance of information sharing, including the intelligence information flow between the government and industry, in relation to protecting critical infrastructure was also addressed in the report.

EO 13636 and PPD-21 demonstrate the U.S. government’s commitment to support and enhance the information sharing process.

Chapter 2 – Current State of Security Clearances

Overview
This chapter discusses the current state of security clearances (including the process of obtaining a clearance and some of the challenges therein), the various federal government departments and agencies that sponsor clearances, and the requirements to which applicants and clearance holders must adhere.

Many industry members obtain clearances through the PSCP, which was established specifically to sponsor clearances for private sector partners responsible for CIP issues. Currently, the PSCP holds many Secret clearances for Electricity Sub-sector personnel, and but only three Top Secret clearances for the entire Energy Sector.

Current Protocols for Granting Clearances
Clearance-Holding Organizations
Several federal government departments and agencies sponsor security clearances for industry representatives; however, the PSCP specifically sponsors clearances for private sector partners who are responsible for CIP but would not otherwise be eligible for a clearance under EO 12829. These partners are SMEs within specific industries and sectors.

While the PSCP is the most appropriate program for facilitating security clearances, individuals may seek out other federal government departments and agencies that also sponsor clearances. This diversity could allow more clearances to be processed during the same time period and may offer more Top Secret clearances. Regardless of the organization, the sponsoring department or agency pays for the clearance process; private sector companies cannot pay the costs to process clearances.

PSCP Process
Like all other federal government departments and agencies, the PSCP requires individuals to complete clearance request forms to initiate the process. The PSCP clearance request form is signed by both the federal official who nominated the applicant and the Assistant Secretary for Infrastructure Protection. Upon approval to process, the PSCP administrator contacts the nominee to obtain additional data, which is then submitted for investigation processing. The applicant is required to complete an online security questionnaire and submit fingerprint cards. If the applicant passes a preliminary background check, he or she is granted an interim clearance and then enters the investigation phase, which includes a full investigation and adjudication. If the applicant passes the investigation phase, he or she will have completed the clearance process and must then complete initial training, which includes signing materials and non-disclosure agreements prior to finalization of the clearance holder’s record in the DHS database.

One challenge industry faces in working through the PSCP is excessive processing time. The PSCP manages clearances for individuals across all 16 critical infrastructure sectors, not just the Energy Sector. Therefore, applicants must be mindful of processing their paperwork in a timely manner since many critical infrastructure applicants may be in the queue at any one time. Another challenge industry faces is the limited number of Top Secret clearances currently available to industry through the PSCP. The PSCP offers three Top Secret clearances to the Electricity Sub-sector.

In November 2011, the PSCP was temporarily shut down, which halted clearance processing for industry and restricted the information sharing structure that had been developed over the years through the program. While the program has been reinstated and is working to address the backlog, the shutdown exposed challenges with the current model. This report contains several recommendations that will assist the PSCP by offering potential solutions to the challenges the PSCP faces.

The current PSCP process for obtaining a security clearance is outlined in Appendix II. The PSCTF suggests that (1) organizations work with their CIPC representatives and the ES-ISAC to tailor the model outlined in Chapter 4 (and Figure 1) to the organization’s specific needs, (2) work through their CIPC representatives to ensure the organization is nominating the appropriate industry SMEs and executives, and (3) coordinate with the ES-ISAC to assist with submitting clearance applications to the PSCP.

14 See Appendix II for more information.
Applicant and Clearance Holder Requirements
In addition to the challenges associated with the clearance process, applicants and clearance holders create their own set of obstacles. For example, DHS has noted that many applicants do not complete their online questionnaires or fail to do so in a timely manner, which can further delay or suspend the process. Clearance applicants must be prepared to provide a significant amount of background information, generally dating back 10 years.

Once granted a DHS-sponsored clearance, clearance holders must also complete the private sector annual training requirements. If the clearance holder does not complete the required training, he or she no longer meets the qualifications and the clearance may be deactivated. Individuals who change jobs within their organization or sub-sector and still require access to classified information may retain their clearances but must immediately notify the PSCP of the job change.
Chapter 3 – Setting Expectations and Establishing Guidance

Overview
With respect to the challenges outlined in Chapter 2, industry members who seek to obtain and use security clearances must have a clear understanding of what is expected of them during the entire application process and what classified activities they must perform once they have been granted clearances. Individuals with security clearances have certain responsibilities and obligations beyond their companies that benefit the entire sector.

Unfortunately, many clearances holders do not use their clearances to the greatest extent possible, either due to lack of understanding about how to use their clearances or lack of available information sharing opportunities. In some cases, clearance holders stated that they were unsure of how to use the information from classified briefings; others found that the information provided was not timely or actionable.

The greatest value of the program lies in the opportunity for industry to share its vision with government partners so that the sectors can truly benefit. These ideas may be limited to what the sub-sector can do internally to simplify some aspects of the process. Industry can provide clearer guidance to the government regarding prioritization of job functions and applicants, as well as a method for tracking actively and inactively used clearances.

Develop Priority Guidance for Organizations
Since DHS (and other federal government departments and agencies) processes clearance applications on a first-in, first-out basis, organizations should use the proposed guidance and clearance model in Chapter 4 of this report to identify and prioritize the individuals (including the number of individuals) to be considered for clearance application, then work with their CIPC representatives and the ES-ISAC to facilitate clearance submissions to the DHS PSCP. The guidance is based on, but not limited to, the following criteria: size of the organization, the organization’s functional registration, and criticality of the organization’s assets. When the number of applicants is constrained by limits within the PSCP, organizations should give additional priority to individuals with the job functions and industry involvements that will benefit the most from clearances.

The PSCTF recommends that the ESCC review and approve the prioritization guidelines. Once approved, the ESCC should communicate the sector’s prioritization guidelines to the Energy GCC. The ESCC should identify the ES-ISAC as the sector’s point of contact to facilitate processing nominations for the clearance application process. The full process is outlined in Appendix II.

The PSCTF encourages organizations to coordinate with their CIPC representatives so that the ES-ISAC can facilitate submission to the PSCP (see Chapter 4).

Prior to nominating a candidate for security clearance, each BPS entity should consider several basic questions:

1. Will the nominee be able to use the security clearance to the benefit of both the BPS entity and the government–industry information sharing program? The entity should consider if the nominee (1) has the necessary skills and expertise, (2) is ready and available to respond to requests or incidents, and (3) has the organization’s authorization to share sensitive information.
2. Will the BPS entity support the time and resources necessary for the nominee to participate in classified briefings and other information sharing activities away from their primary duties?
3. Will the nominee have access to a local government facility where classified information can be disseminated for review and discussion, or will the cleared individual be allowed and willing to travel to cleared government facilities for the purposes of reviewing and sharing classified information with government SMEs?
   Note: Examples of cleared facilities include local FBI offices, Federal Aviation Administration offices at major airports, Department of Defense facilities, Secret Service offices, and DHS/State fusion centers.
4. Is the nominee willing to dedicate the additional time and travel needed to participate in ongoing information sharing opportunities with government partners? Note: These opportunities could include attending cleared regional briefings and discussions with local FBI and other LEAs. Additional meetings may be conducted at various federal government department and agency locations in Washington, DC.
5. Will the nominee and the BPS entity support the ES-ISAC’s classified activities and discussions, be available to respond immediately to incidents, and help develop industry alerts and advisories?
6. Will the nominee maintain his or her current job function for a sufficient period of time (i.e., three years) to warrant the resources, time, and effort needed to obtain a U.S. government security clearance?
7. Is the nominee willing to participate in the required background evaluation? Note: The applicant must be prepared to provide a significant amount of personal background, financial, and educational information (generally dating back 10 years) to complete the government investigations needed to obtain a U.S. government security clearance. The application and adjudication process may take from six months to a year or more before a clearance is issued.

**Designate the Appropriate Individuals**

To ensure clearances are used to the greatest extent possible, organizations should develop criteria that will allow clearances to be assigned to job functions or individuals with the greatest need first. Each organization should review its operational structure to determine which individuals are best positioned to: participate in cleared briefings, provide subject matter expertise to the IC, share potentially sensitive information from their organization, motivate their organizations to take action based on the information provided, exercise appropriate discretion with the classified material, and influence others in their organizations to change security postures based on available information.

Organizations should refer to the industry clearance model (presented in Figure 1) to determine which functional entities and areas of expertise most accurately reflect their requirements for clearances: Cybersecurity, Physical Security, Operational Security, or Executive. Figure 1 outlines various areas of expertise and prioritizes the requests based on the needs of the functional entities.

Organizations should also consider establishing a Security Clearance Coordinator function. This function may assist with developing, implementing, and managing the policies and procedures that the organization would utilize internally. Specific functions may include:

- Helping an organization use the industry clearance model (Figure 1) or other decision-making tools;
- Supporting the clearance process for new and existing clearance holders and applicants;
- Reiterating expectations of use; and
- Coordinating efforts for briefings and general business continuity and redundancy of the security clearance function within an organization.

As a general practice, but with specific focus on maintaining data about cleared personnel, an organization should have policies and procedures in place to protect any personally identifiable information (PII) of clearance holders.15

**Know the Process**

After the organizations and CIPC identify candidates, the candidates may apply for U.S. government security clearances through the appropriate federal government department and agency program (e.g., the PSCP). Applicants may either nominate themselves or coordinate with their local DHS protective security advisor to obtain and complete a DHS Form 9014 for a DHS-sponsored clearance.

Employees should be aware that the clearance process requires individuals to submit detailed personal, professional, educational, and financial information. The individual should be comfortable with an investigator examining these and other areas. If an investigator discovers information that eliminates the individual from further consideration, this rejection could impact the individual’s employment.

**Gather Personal Data in Advance and Adhere to Deadlines**

Throughout the clearance process, applicants must adhere to certain deadlines and time frames. Failure to meet these deadlines will result in the clearance application being delayed—even declined and removed from the processing queue. As such, applicants must be educated about the process and made aware of these deadlines before applying. Additionally, nominees should be encouraged to have all relevant materials prepared in advance of submitting the clearance application.

15 DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Attend Briefings and Establish Contacts
Clearance holders are expected to attend classified briefings whenever possible. Attending briefings positions industry to make the best use possible of the limited number of clearances and allows individuals to make other cleared contacts, which enhances information sharing. Clearance holders should also reach out to their local fusion centers, FBI field offices, Secret Service offices, and other Federal partners to identify where secured briefing facilities exist within their local areas. Finally, clearance holders should coordinate with these local partners and their clearance holders to “perm-cert” their clearance to these local briefing facilities. Having one’s clearance already in place at a local briefing facility, where secure phone and email exchanges can occur, will expedite the flow of critical information when the need arises.

Another CIPC task force, the Information Sharing Task Force (ISTF), is exploring different methods of information sharing among industry members and between industry and government. The ISTF’s report will provide detail on some of the tools and mechanisms by which clearance holders can obtain and share classified information.

Using Classified Information – Parallel Construction
Cleared individuals may not always know how to use the information they receive during a classified briefing. Classified information cannot be disclosed or discussed outside secure places, nor may classified information be discussed with those without security clearances. Therefore, clearance holders must protect the status of classified information that may or may not be in the public domain, and they can neither confirm nor deny whether specific elements of information are classified. Strategic improvements to utility security may often be implemented by obfuscating the individual classified threat information precipitating the change. If unclassified information in the public domain can be used to develop a parallel understanding of the threat, then a clearance holder can take direct action, using that unclassified open source as justification, but without disclosing whether the information is classified or not. This parallel construction provides a way to prioritize which threats the utility should address first without compromising classified information or sources.

Some examples of open source information are the United States Computer Emergency Readiness Team bulletins or NERC Alerts that indicate a need for action, but do not reveal specific classified information. These reports may be based on classified intelligence, but only include details at the FOUO level. Also, news media posts of recent events or attacks can be used, but the fact that the media post is tied to classified information can never be revealed outside classified spaces to those who do not hold U.S. government security clearances. The PSCTF recommends that cleared individuals review their clearance training material thoroughly before attempting to develop parallel construction.

Utility employees with security clearances are expected to integrate their threat analysis efforts with the ES-ISAC to maximize parallel construction potential. Organizations can take immediate tactical action against open source threats and implement longer-term strategic and policy improvements based on classified material regarding advanced persistent threat (APT) actors.

Register and Pass Clearances
Small utilities are normally registered for only one or two of the NERC functions listed in Figure 1, while larger utilities may be registered for multiple functions. Given the segregation of Transmission and Generation functions by Federal Energy Regulatory Commission (FERC) regulations, little opportunity exists for security SMEs in these separate groups to cross-coordinate between various business lines within the same utility. Other large utilities may be segregated and registered as separate business organizations across multiple states to satisfy state regulatory requirements. Each utility should maintain a roster of individuals who hold U.S. security clearances and which functional areas and skill sets each person represents. The PSCTF recommends that the utility hold any roster that identifies clearance holders or includes PII as restricted information, according to the company’s protection of sensitive information policies.

Exceptions for additional DHS-sponsored clearances that exceed the allocated numbers found in Figure 1 (per utility) should be rare and will be coordinated among the organization, CIPC, the ES-ISAC, and the PSCP point of contact on a case-by-case basis.

The PSCTF believes there is an opportunity for clearance-granting federal government departments and agencies within the federal government to better coordinate the clearance process, including passing clearances from one department to the

---

16 Permanent Certification, or “perm-cert,” allows a person who is cleared through one U.S. federal department or agency to have their clearance passed to another U.S. federal department or agency for a period of up to one year.

17 See the Information Sharing Task Force report for details on information sharing opportunities.

next for briefing purposes. Currently, several government systems maintain the personnel security records of clearance holders across various departments and agencies. These systems include Scattered Castles, the Joint Worldwide Intelligence Communications System, the Integrated Security Management System, and the Joint Personnel Adjudication System. Reconciling the different systems would increase clarity and ease efforts in passing clearances between departments and agencies.

Chapter 4 – Clearance Model for Industry

Model Overview

The PSCTF recommends that industry organizations use the model described in this section to manage their overall need for security clearances. The goal in using this model is to align with and support the missions of NERC and the U.S. government. As stated previously, the intent of developing and using this model across industry is to provide appropriate industry SMEs and executives security clearances based on balanced NERC Functional Entity Registration Type, SME, and executive-level criteria.

The proposed clearance model is based on an organization’s registrations within the NERC Reliability Functional Model as a guide for the maximum number of security clearances needed, and should provide a means for scaling across the diverse set of utility configurations within industry. Each organization should have four cleared staff members for each registration type. For large, complex organizations, a more appropriate solution may be that each operating company nominates four individuals from different areas of expertise. To understand and effectively respond to dynamics around critical infrastructure threats, cleared personnel must have the expertise and authority to make decisions in regard to cybersecurity, physical security, and system operations. In addition, an executive-level role is needed to provide priority support for both policy and strategic components of a comprehensive security plan. Those individuals responsible for the security of the BPS and supporting ancillary systems must be prioritized for clearances.

Areas of expertise include security of assets that are essential to support reliable operations such as:

- Energy Management Systems (EMS);
- Supervisory Control And Data Acquisition (SCADA) and Control Systems and supporting Auxiliary Systems;
- Advanced Metering Infrastructure;
- Physical security;
- Cybersecurity;
- BPS Situational Awareness systems; and
- Other cyber assets found in the utility enterprise infrastructure that support maintenance and restoration of above the systems and assets.

The goal is to manage the clearances within the organization to minimize the chance of information silos that may create security vulnerabilities. Depending on the organizational structure, individuals with similar skill sets may require security clearances to protect the overall enterprise systems and specific systems throughout the various business units. This requirement will vary from organization to organization.

Using the Model

Select Job Functions

When determining clearances for individuals, an organization must consider its functions and the infrastructure elements and systems it is responsible for protecting. Figure 1, below, is a guideline that will help organizations ensure coverage by identifying appropriate executives and SMEs dealing with cybersecurity, physical security, and operations.

The job functions are described as follows:

- Executives – Corporate officers, directors, and senior managers of an organization who have comprehensive enterprise security and risk management responsibilities. These executives should have decision-making authority in terms of BPS operations and be in a position to effect change, authorize expenditures, exercise formal policy approval, accept fiduciary responsibility, and be available for immediate contact. These qualifications are critical when actionable intelligence must be acted on, but the details cannot be shared outside of the classified spaces.

Registrations include: Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), Transmission Owner (TO), Transmission Service Provider (TSP), Generation Operator (GOP), Generation Owner (GO), Distribution Provider (DP), and Interchange Coordinator (IC).
- **Cybersecurity SMEs** – Individuals who understand the organization’s cyber systems and how they interact with various functional areas, both vertically and horizontally, and have the skills, authority, and focus regarding the enterprise system and functional subsystems (e.g., corporate networks, EMS/SCADA, Generation and Transmission control, and Market Management Systems linked to EMS/SCADA).

- **Physical Security SMEs** – Individuals who understand the organization’s physical systems and have the skills, authority, and focus regarding the enterprise system and functional subsystems. Example job titles or descriptions are chief security officers, directors of security operations centers, and managers of physical security guard forces.

- **Operational SMEs** – Individuals who are able to affect real-time operations and make decisions on operating posture based on emerging threat information.

### Maximum Number of Clearances

The PSCTF recommends four cleared people per organization (or per NERC’s registered function), one person covering each of the job descriptions listed in Figure 1 below. Some companies will require fewer cleared personnel; some companies will require more cleared personnel. For the latter, the organization should prioritize the initial four candidates, as noted in Figure 1. The PSCTF also recommends that organizations work with their CIPC representatives and the ES-ISAC to tailor the guidance in this report to each organization and to prioritize (by job function) those personnel requiring clearances. Figure 1 also serves as a helpful guide for tracking an organization’s overall clearances.

**Figure 1: Clearance Model for Industry**

<table>
<thead>
<tr>
<th>AREA OF EXPERTISE</th>
<th>NERC FUNCTIONAL ENTITY REGISTRATION TYPE*</th>
<th>Total</th>
<th>Granting Department or Agency (DOE, DHS, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>RC</td>
<td>BA</td>
<td>TO</td>
</tr>
<tr>
<td>Jane Doe*</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Physical Security</td>
<td>RC</td>
<td>BA</td>
<td>TO</td>
</tr>
<tr>
<td>Jane Smith*</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Operations</td>
<td>RC</td>
<td>BA</td>
<td>TO</td>
</tr>
<tr>
<td>John Smith*</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Executive</td>
<td>RC</td>
<td>BA</td>
<td>TO</td>
</tr>
<tr>
<td>John Doe*</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

* Reliability Coordinator (RC), Balancing Authority (BA), Transmission Owner (TO), Transmission Operator (TOP), Transmission Service Provider (TSP), Generation Operator (GOP), Generation Owner (GO), Distribution Provider (DP), and Interchange Coordinator (IC).

* Priority personnel

^ Second level priority personnel
Chapter 5 – Findings and Recommendations

Findings
The recommendations below are based on the PSCTF’s findings with respect to the need for additional clearances within the Electricity Sub-sector. Additional clearances assigned to appropriate areas of expertise will allow cleared individuals to better understand and act on classified information regarding the reliability, security, and resilience of the BPS.

The PSCTF finds that:

- Industry subject matter expertise provides valuable operational context for information that might otherwise be overlooked or undervalued by the IC.\(^{21}\)
- Industry does not have a consistent process to identify appropriate individuals for clearances. Organizations may have their own processes, but they lack the consistency to optimize the distributions of clearances across functional SME groups and ensure adequate executive participation.
- The classified information sharing process is maturing from a government-led, one-way briefing for a small number of cleared industry personnel to a collaboration of government–industry experts in the classified space. Information sharing challenges arise because industry lacks a sufficient number of individuals with the skills, background, or authority for clearances.
- Clearance holders need to be better informed about the clearance process and requirements.
- For the information sharing process to be effective, industry needs to increase the number of appropriate individuals with clearances who actively participate.
- Due to specific skill sets and operational activities required to engage in highly classified settings such as the NCCIC, additional industry SMEs must be cleared at the TS-SCI level.

Recommendations
In response the PSCTF’s findings above, the following recommendations are provided for ESCC consideration:

1. The ESCC should work closely with the government to inform public partners of the subject matter expertise that industry experts bring to classified discussions at the policy and strategic level. The ES-ISAC should work closely with the IC to inform public partners of the subject matter expertise industry experts bring to classified discussions at the operational level.
2. The CIPC should coordinate with industry organizations to implement the functional model proposed in this report. The model will help organizations identify job positions that could benefit the reliable operation of the BPS if incumbents would obtain security clearances and participate in classified information sharing discussions. In addition, industry organizations should work with the ES-ISAC to facilitate the submission of industry requests for security clearances into the PSCP queue.
3. The ES-ISAC should facilitate industry assistance to DHS by providing information about necessary skills, background, and authority of clearance applicants to make the PSCP more responsive to industry needs.
4. The CIPC should encourage clearance nominees to use the guidance in this report to streamline their participation in the PSCP application process.
5. The CIPC and ESCC should set clear expectations about clearance holders attending classified briefings and cleared workshops and meetings with government officials. For example, clearance holders should:
   b. Increase use of the ES-ISAC.
   c. Coordinate with the IC and LEA field offices.
   d. Complete annual training requirements.
   e. Notify the PSCP of personnel change actions that affect job tasks and scope of responsibilities.

6. The ESCC should request additional TS-SCI clearances from the GCC for ES-ISAC personnel to staff the NCCIC and for SMEs with specific skill sets that will populate the ES-ISAC Hydra network.

7. The ESCC should recommend that the federal government reconcile by sector the different personnel records systems to increase clarity and ease efforts in passing clearances between departments and agencies. Currently, several government systems maintain the personnel security records of clearance holders across various departments and agencies. Reconciling these systems by sector would resolve duplication or challenges in passing clearances.
Appendix I: Other Federal Departments and Agencies that Sponsor Clearances

Fusion Centers
Chapter 2 of this report discussed DHS’s PSCP and its relationship with the Electricity Sub-sector. In addition to the PSCP, state and major urban area fusion centers also sponsor clearances, generally at the Secret level. Fusions centers serve as primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal, state, local, tribal, and territorial partners. Located in states and urban areas throughout the country, fusion centers allow front-line law enforcement, public safety, fire service, emergency response, public health, CIP, and private sector security personnel to lawfully gather and share threat-related information. They provide situational awareness, conduct analyses, and facilitate information sharing to help prevent, protect against, and respond to crime and terrorism.

Federal Government Departments and Agencies
Several other federal government departments and agencies sponsor clearances for the private sector. According to EO 12968, Access to Classified Information, security clearances are only granted to persons:

Employed by, detailed or assigned to, an [executive] agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

Departments and agencies, such as the Department of Defense, the Department of Energy, and the Department of Justice can sponsor and hold security clearances for private sector individuals.

One-Day Read-Ins
In some instances, certain federal government departments and agencies permit uncleared individuals to attend classified briefings by allowing the individuals to be read in for a 24-hour period. For example, the Enduring Security Framework—an effort that brings together technology and defense company senior executives and top officials from the Department of Defense, Department of Homeland Security, and the Director of National Intelligence—mobilizes government and industry experts to identify vulnerabilities and address security risks. Cases that would allow for this type of read-in include special security briefings in which decision-makers or SMEs need access to specific information to address a threat or vulnerability.

---

23 Ibid.
Appendix II: Security Clearance Process

The following process is the PSCTF’s proposed clearance process. Much of it is based on existing models, with more involvement of the NERC CIPC and the ES-ISAC.

Identification Phase (2 weeks)
Applicants for security clearances from the Electricity Sub-sector may either nominate themselves to the energy sector specialist within the Partnership Outreach Division (POD) of the DHS or coordinate with their local DHS/PSA (Protective Security Advisor) to obtain and complete a DHS Form 9014.

These NERC guidelines will now require applicants to clearly state in the remarks section of the DHS Form 9014 which functional area (by NERC registration number) and SME skill set they represent. This information should be obtained from the utility functional security coordinator or manager who has oversight of the security clearance holders within each utility. The applicant will also have to provide information on why he or she should receive the clearance.

The energy sector specialist (ESS) will review the applicant’s information and validate the applicant’s need to know for access to U.S. government classified information. Eligible applicants will be employees of the reference utility—not contractors or consultants. No exceptions will be granted under the DHS PSCP.

DHS-sponsored clearances are nominally granted at the Secret level only to industry participants who meet certain criteria and have successfully completed the DHS clearance process. Applicants who are not verified as electric utility employees or are without valid need for access to classified information may be denied by the ESS or DHS/IP leadership at this step.

Approval Phase, Part 1 of 2 (1 week)
Once a valid DHS Form 9014 is received, the ESS will verify the basic information on the form and coordinate with the ES-ISAC for questions about the applicant, the applicant’s need to know, or the organization requesting the clearance. The ESS screens the form with the ES-ISAC to ensure that the applicant is a current employee of an Electricity Sub-sector utility and that the organization is not exceeding the maximum four DHS-sponsored clearance holders within a functional area at a particular utility. In cases in which the number of clearance holders requested exceeds the number recommended by the clearance model, the ESS may seek additional justification and validation from the utility or the ES-ISAC for additional clearance holders at that utility, or deny the clearance. The applicant is notified if he or she does not meet the criteria for further processing.

Approval Phase, Part 2 of 2 (1–2 weeks)
The validated DHS Form 9014 is then passed to the PSCP administrator who validates the information and presents the information to the POD leadership for review and approval. The PSCP administrator may request additional information or justification from the applicant, utility, or NERC, if needed. The ESS (or the PSCP administrator) will set up a phone call during which the applicant will provide additional PII (i.e., Social Security Numbers), which should not be transmitted in clear text via email over the Internet. The completed DHS Form 9014 is returned to the PSCP administrator for clearance processing.

Pre-Investigation Phase, Part 1 of 2 (2–4 weeks)
Once the PSCP administrator has the PII, he or she will initiate eQIP access for the applicant. The PSCP administrator will send out a welcome package with unique eQIP links and mail the applicant DHS fingerprint cards and release forms for completion. The applicant will complete the forms and fingerprint cards at a local LEA office and return them to the PSCP administrator. The applicant will also need to complete the eQIP process online and ensure that the PSCP administrator reviews the information for completeness and accuracy. The PSCP administrator will follow up with the applicant as needed to ensure completion of the process.

Pre-Investigation Phase, Part 2 of 2 (2–4 weeks)
Upon receipt of the completed DHS fingerprint cards, the PSCP administrator will send them to DHS Personnel Security Division (PSD) where they will be scanned and archived. Upon completion of the eQIP process and receipt of DHS fingerprint cards, DHS PSD will initiate a preliminary investigation of the applicant.

27 eQIP is the name of the U.S. government system used to collect and manage clearance applicant information.
Investigation Phase, Part 1 of 2 (4–8 weeks)
If the applicant passes the preliminary investigation background check, PSD will normally grant an interim clearance, which is accepted by some federal government departments and agencies but not all. If the clearance was denied, the PSD will notify the Applicant that they do not meet the criteria for access; the PSCP administrator, sector specialist, and PSA will be also notified of the denial. This information is not public.

Investigation Phase, Part 2 of 2 (4–8 weeks)
The PSD will send applicants that pass the preliminary investigation background check to the Office of Personnel Management for a full investigation and adjudication of any necessary items. The PSCP administrator will send interim clearance notices to the applicants as well as initial training materials and non-disclosure agreements that must be completed prior to completing their interim clearance records.

Adjudication Phase, Part 1 of 2 (12–15 weeks)
If the Office of Personnel Management needs more information, it will contact the DHS PSD to complete the full investigation. The office will send the final results back to PSD for final adjudication and the subsequent notification to the applicant that the final clearance has been completed.

Adjudication Phase, Part 2 of 2 (12–15 weeks)
If the final clearance is not approved, the DHS PSD will notify the PSCP administrator that the clearance has been denied, and the PSCP administrator will update the records to reflect this. The DHS PSD will also notify the sector specialist and/or PSA who nominated the applicant that the clearance has been denied. Finally, the DHS PSD will notify the applicant of the denial.

Final Notification and Initial Training
The DHS PSD will notify the PSCP administrator that the clearance has been approved, and the PSCP administrator will update and store the clearance information with DHS database archives. The DHS PSD will notify the sector specialist and/or PSA who nominated the applicant for the clearance. Finally, the DHS PSD will notify the applicant that they have successfully completed the clearance process.

If the applicant, now clearance holder, has not been previously granted an interim clearance, he or she must complete initial training materials and non-disclosure agreements prior to finalization of the clearance holder’s record in the DHS database.

Annual Training Requirements
The DHS PSCP administrator will provide and track the successful completion of annual training by all DHS clearance holders. If the clearance holder does not complete the annual training or no longer meets qualifications, the clearance may be deactivated. In situations in which the clearance holder remains within the Electricity Sub-sector, they may retain their clearances so long as the need for access to classified information remains valid.

Attending Classified Briefings
Clearance holders will contact the PSCP administrator when there is a need to attend a classified meeting or briefing. The clearance holder will complete a DHS Form 1100-7, and the PSCP administrator will send the completed form to DHS customer service to be forwarded to the department or agency hosting the briefing.

If the briefing is sponsored by DHS/IP, the PSCP will work with the sector specialist and others at the host facility security function to record attendance and brief authorized participants.

If DHS/IP does not sponsor the briefing, then DHS customer service will send messages or memos to the Office of Security for the department or agency hosting the briefing or meeting. DHS customer service notifies PSCP administrator that the clearance has been passed to the hosting organization.

The clearance holder will comply with all security restrictions and instructions provided by the hosting department or agency with respect to the protection and safeguarding of information shared by the government with the industry
participants. The hosting organization will provide specific instructions on accepted behavior while in the cleared facility and subsequent use of classified information learned during the cleared session.