United States Government Accountability Office

Report to Congressional Committees

February 2017

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts

Accessible Version

GAO-17-182

GAO Highlights

Highlights of GAO-17-182, a report to congressional committees

February 2017

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts

Why GAO Did This Study

Critical infrastructure protection access controls limit access to those with a legitimate need. DHS is the lead federal agency for coordinating critical infrastructure protection efforts with other federal agencies, and partnering with nonfederal stakeholders. The National Defense Authorization Act of 2016 included a provision for GAO to review critical infrastructure access control efforts.

This report examines (1) key characteristics of selected federally-administered critical infrastructure access control efforts and factors that have an impact on stakeholders' use of them; (2) the extent to which DHS has taken actions to harmonize efforts across critical infrastructure sectors; and (3) the extent to which DHS's SCO has taken actions to harmonize access control efforts across DHS. GAO examined six federally-administered access control efforts across three federal departments. Efforts were selected, among other things, to represent a range of efforts that groups of users—such as truck drivers—may encounter while accessing multiple facilities. GAO interviewed DHS, NRC, and DOD officials and users and operators affected by the efforts and reviewed relevant documents.

What GAO Recommends

GAO recommends that (1) DHS work with partners to identify any opportunities to harmonize access control efforts across critical infrastructure sectors and (2) SCO establish goals and objectives to support its broader strategic framework for harmonization. DHS concurred with both recommendations.

View GAO-17-182. For more information, contact Chris P. Currie at (404) 679-1875 or CurrieC@gao.gov.

What GAO Found

The six selected federally-administered critical infrastructure access control efforts GAO reviewed generally followed similar screening and credentialing processes. Each of these efforts applies to a different type of infrastructure. For example, the Transportation Security Administration's Transportation Worker Identification Credential controls access to ports, the Department of Defense (DOD) Common Access Card controls access to military installations, and the Nuclear Regulatory Commission (NRC) regulates access to commercial nuclear power plants. GAO found that selected characteristics, such as whether a federal agency or another party has responsibility for vetting or what types of prior criminal offenses might disqualify applicants, varied across these access control efforts. In addition, these access control efforts generally affect two groups of stakeholders—users and operators—differently depending on their specific roles and interests. Users are individuals who require access to critical infrastructure as an essential function of their job; while, operators own or manage facilities, such as airports and chemical facilities. Regardless of infrastructure type, users and operators that GAO interviewed reported some common factors that can present challenges in their use of these access controls. For example, both users and operators reported that applicants requiring access to similar types of infrastructure or facilities may be required to submit the same background information multiple times, which can be costly and inefficient.

The Department of Homeland Security (DHS) relies on partnership models to support collaboration efforts among federal and nonfederal critical infrastructure stakeholders, but has not taken actions to harmonize federally-administered access control efforts across critical infrastructure sectors. According to DHS officials, these partnerships have not explored harmonization of access control efforts across sectors, because this has not been raised as a key issue by the members and because DHS does not have a dedicated forum that would engage user groups in exploring these issues and identifying potential solutions. DHS's partnership models offer a mechanism by which DHS and its partners can explore the challenges users and operators may encounter and determine opportunities for harmonizing the screening and credentialing processes to address these challenges.

DHS's Screening Coordination Office (SCO) has taken actions to support harmonization across DHS access control efforts, but it has not updated its goals and objectives to help guide progress toward the department's broader strategic framework for harmonization. SCO's strategic framework is based on two screening and credentialing policy documents—the 2006 Credentialing Initiative Report and 2008 Credentialing Framework Initiative. According to SCO officials, they continue to rely on these documents to provide their office with a high-level strategic approach, but GAO found that the goals and objectives outlined in the two documents are no longer current or relevant. In recent years, SCO has helped the department make progress toward its harmonization efforts by responding to and assisting with department-wide initiatives and DHS component needs, such as developing new programs or restructuring existing ones. However, without updated goals and objectives, SCO cannot ensure that it is best supporting DHS-wide screening and credentialing harmonization efforts.

Contents

Tables

Figure

Abbreviations

CAC	Common Access Card

CFATS	Chemical Facility Anti-Terrorism Standards
CFI	Credentialing Framework Initiative
CIPAC	Critical Infrastructure Partnership Advisory Council
CIR	Credentialing Initiative Report
DHS	Department of Homeland Security
DOD	Department of Defense
GCC	Government Coordinating Councils
HME	Hazardous Materials Endorsement
HSPD	Homeland Security Presidential Directive
IP	Office of Infrastructure Protection
ISC	Interagency Security Committee
MMC	Merchant Mariner Credential
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
NRC	Nuclear Regulatory Commission
PADS	Personnel Access Database System
PPD	Presidential Policy Directive
SCC	Sector Coordinating Councils
SCO	Screening Coordination Office
SIDA	Secure Identification Display Areas
SSA	Sector-Specific Agency
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

February 7, 2017

Congressional Committees

The nation's critical infrastructure—systems, facilities, assets, and networks provide the essential services that serve as the backbone of our nation's economy, security, and health—could be attacked by those who seek to harm the United States and its interests. Strengthening and maintaining secure, functioning, and resilient critical infrastructure requires proactive and coordinated efforts. This endeavor is a shared responsibility among federal, state, local, tribal, and territorial entities, and public and private owners and operators of critical infrastructure. One aspect of maintaining secure critical infrastructure is access control—that is, limiting the access to physical facilities and assets to only those who have a legitimate need and have been vetted to ensure there is no evidence that they pose a risk. Although the federal government owns little of the nation's critical infrastructure, federal agencies play various roles—in partnership with nonfederal stakeholders—to help ensure effective access control efforts that do not unnecessarily impede the flow of legitimate business and operations.

The Department of Homeland Security (DHS) is the lead federal agency responsible for overseeing domestic critical infrastructure protection efforts, but other federal agencies are responsible for overseeing different sectors of critical infrastructure, such as the defense industrial base sector and the energy sector. DHS's National Infrastructure Protection Plan (NIPP),[1] outlines the roles and responsibilities of DHS and sector-specific agencies (SSA)—federal departments and agencies responsible for critical infrastructure protection and resilience activities across 16 critical infrastructure sectors.[2] In 2006, in response to Homeland Security Presidential Directive/HSPD-11 (HSPD-11) DHS established the Screening Coordination Office (SCO), located within DHS's Office of

[1] See DHS, *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013), which is an update to previous versions of the NIPP.

[2] The 2013 NIPP identifies the 16 critical infrastructure sectors: (1) Agriculture and Food, (2) Chemical, (3) Commercial Facilities, (4) Communications, (5) Critical Manufacturing, (6) Dams, (7) Defense Industrial Base, (8) Emergency Services, (9) Energy, (10) Financial Services, (11) Government Facilities, (12) Healthcare and Public Health, (13) Information Technology, (14) Nuclear Reactors, Materials and Waste, (15) Transportation Systems, and (16) Water and Wastewater Systems.

Policy.[3] SCO is responsible for overseeing DHS's screening and credentialing activities, including those aimed at critical infrastructure access control efforts. "Credentialing," in this context, refers to the entire process of determining a person's eligibility for a particular license, privilege, or status, from application for access through issuance, use, and expiration or potential revocation of an issued credential.

Federally-administered access control efforts generally involve two groups of stakeholders: users and operators. Users are individuals who require access to critical infrastructure as an essential function of their job. Operators own or are responsible for managing facilities, such as airports, seaports, and chemical facilities, which are generally privately owned, but can also include government facilities such as military installations.

The National Defense Authorization Act for Fiscal Year 2016 included a provision for us to report on the background check, access control, and credentialing requirements of federal efforts for the protection of critical infrastructure and key resources, with an emphasis on harmonization—identifying and implementing opportunities to enhance efficiency within or across related processes—by enhancing interoperability and reducing redundancy.[4] This report (1) describes key characteristics of selected federal critical infrastructure access control efforts and factors that have an impact on stakeholders' use of them; (2) examines the extent to which DHS has taken actions to harmonize federally-administered access control efforts across critical infrastructure sectors; and (3) examines the extent to which DHS's Screening Coordination Office has taken actions to harmonize critical infrastructure access control efforts across the department.

To answer our first objective, we examined six federally-administered access control efforts across three federal departments—DHS, the Department of Defense (DOD), and the Nuclear Regulatory Commission (NRC). We focused on efforts that (1) were regulated or guided by the federal government and (2) facilitated access to physical facilities or

[3] See *Homeland Security Presidential Directive 11: Comprehensive Terrorist-Related Screening Procedures*/HSPD-11 (HSPD-11) (Aug. 27, 2004). HSPD-11 defines terrorist-related screening as the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. It also includes risk assessment, inspection, and credentialing.

[4] Pub. L. No. 114-92, tit. X, § 1086(f)(11), 129 Stat. 726, 1011-12 (2015).

assets.[5] The six federal access control efforts included are: Transportation Worker Identification Credential (TWIC), Hazardous Materials Endorsement (HME), Secure Identification Display Area (SIDA), Common Access Card (CAC), Chemical Facility Anti-Terrorism Standards (CFATS), and Commercial Nuclear Power Plant Regulations (NRC).

To select the access control efforts, we initially focused on DHS-administered programs and reviewed DHS's 2006 *Credentialing Initiative Report* (CIR).[6] We selected four access control efforts administered by DHS based on our review of the CIR and identified the seven DHS screening and credentialing effort related to access control. Those seven access related efforts are a subset of other DHS credentialing efforts that focused on screening efforts related to access to controlled locations, such as ports or secure areas. We selected three of these seven DHS access efforts because they regulate or facilitate access to critical infrastructure assets.[7] Because the three access control efforts identified from DHS's CIR were related to the transportation sector, we included another effort within DHS, but for another sector—CFATS, which is related to the chemical sector but not included in the CIR because it was implemented after 2006.[8]

[5] Largely, the federal efforts in our review involved access controls to secure physical facilities. However, in one case—the Hazardous Material Endorsement—the particular license, privilege, or status conferred is permission to transport hazardous materials, which, in the wrong hands, could be used to carry out attacks against the United States or its interests. Similarly, in some cases—for example, chemical facilities—in addition to preventing sabotage to, or attacks on the facilities themselves, access controls can limit opportunities for persons with bad intent to obtain, through theft or other means, materials that could be used to carry out an attack.

[6] DHS, Screening Coordination Office, *Credentialing Initiative Report* (Washington, D.C.: December 2006).

[7] The remaining four access efforts were scoped out because they do not regulate or facilitate access to critical infrastructure assets. Armed Law Enforcement Officer relates to the ability of law enforcement officers to be armed and does not provide access to physical critical infrastructure. Merchant Mariner Credentials are a competency-based credential in which vetting is conducted through the Transportation Worker Identification Credential, which is covered in our review. Additionally, the First Responder Access Credential is not a current effort. Finally, Federal worker-ID credential is a government-wide program that is administered by each federal department or agency. We selected the Department of Defense's implementation of the federal worker ID credential, the Common Access Card, as one of the efforts.

[8] CFATS was not operational at the time the 2006 CIR was drafted; therefore it was not included in the list of access control efforts.

To provide context and perspective on government-wide efforts, we also selected federal efforts administered by agencies outside of DHS. To identify these two efforts, we spoke with DHS federal administrators or nonfederal stakeholders related to the four access control efforts we selected above to obtain information on other frequently used access control efforts they identified as relevant to accessing secure critical infrastructure. We included access control efforts administered by DOD and NRC, which are the two federal departments responsible for the access control related to military installations (CAC) and commercial nuclear power plants (NRC regulations), respectively.

Our selection does not represent the universe of federal access control efforts. For instance, the NIPP lists 16 critical infrastructure sectors; while the access control efforts in our review relate to 4 of the sectors: Chemical; Government Facilities (Military Installations); Nuclear Reactors, Materials, and Waste; and Transportation. The results from our selection are not generalizable, but they provide perspectives on organizational structures and operational policies and procedures across different infrastructure types and different federal agencies.

To collect information on the key characteristics of the federal access control efforts in our review, we developed a standard set of questions based on the credentialing and screening phases identified in DHS's 2006 CIR and submitted it to DHS, DOD, and NRC federal administrators. We reviewed relevant regulations, policies and procedures, and interviewed DHS, DOD, and NRC administrators to corroborate the information obtained from the standard set of questions.

To determine the factors that had an impact on stakeholders' use of the access control efforts, we interviewed user and operator stakeholder groups. To identify the types of users and operators that may encounter the federal critical infrastructure access control efforts in our review, we consulted our prior critical infrastructure work, spoke with agency officials from DHS, NRC, and DOD, and reviewed published DHS critical infrastructure documentation. We met with nonfederal stakeholder groups that represented owners and operators who are responsible for managing critical infrastructure facilities, for example, the American Association of Airport Executives. To select associations representing user groups, we limited our selection to users that would regularly require access to multiple types of critical infrastructure, such as truck drivers and skilled trades workers, such as the United Brotherhood of Carpenters.[9] We interviewed the nonfederal stakeholder groups described above to understand the impacts and challenges of our selected access control efforts on stakeholders.

While the sample of stakeholder groups encompasses the six critical infrastructure access control efforts in our review, the cross-section of stakeholder groups we spoke to is a non-generalizable sample. As such, viewpoints expressed by such groups cannot be extended to the entire population of stakeholders. However, the sample allowed us to gain insights into the interests and perspectives of the stakeholder communities related to accessing secure critical infrastructure. Our findings from interviews with nonfederal stakeholder groups cannot be generalized to all users or operators of critical infrastructure facilities but provide useful insight into their experiences and perspectives.

To answer our second objective assessing DHS's actions to harmonize access control efforts across critical infrastructure sectors, we reviewed the 2013 NIPP to identify existing partnership structures designed to enhance collaboration among critical infrastructure stakeholders. We also interviewed officials from the DHS National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection—the lead DHS entity responsible for leading the coordinated effort to secure the nation's critical infrastructure—to determine what actions DHS and its partnership structures have taken to harmonize access control efforts. Additionally, we interviewed DOD and NRC officials to corroborate DHS's external harmonization efforts with these agencies. We compared the actions DHS has taken with its internal guidance governing partnership structures and our prior work on best practices to enhance and sustain collaboration.

To answer our third objective examining SCO's efforts to harmonize access control efforts across DHS, we reviewed the 2006 Credentialing Initiative Report as well as a follow-up report DHS issued in July 2008, which serves as a strategic framework for the department to improve credentialing processes through eliminating redundant activities, leverage investments across programs, and reduce costs of implementing new

[9] The following is the list of nonfederal operator groups that we met with: American Association of Airport Executives, American Association of Port Authorities, American Chemistry Council, American Fuel & Petrochemical Manufacturers, Institute of Makers of Explosives, and Nuclear Energy Institute. The user groups we met with were the American Trucking Associations and United Brotherhood of Carpenters.

capabilities, among other efforts.[10] We also examined, through reviewing documents and interviewing SCO officials, the actions SCO has taken to implement the recommendations outlined in the CIR. We compared SCO's activities and progress toward harmonization goals to *Standards for Internal Control in the Federal Government* to evaluate the extent to which SCO had goal and objectives in place designed to help achieve DHS's broader strategic framework.[11]

We conducted this performance audit from January 2016 to February 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DHS and other federal agencies help administer access control efforts across a wide range of physical facilities and assets in critical infrastructure sectors for which they are responsible. These federal administrators help operators of critical infrastructure assets safeguard the assets against attacks, sabotage, theft, or misuse while facilitating legitimate access to help ensure the flow of business and operations. In efforts to serve operator needs, administrators must also ensure compliance with federal laws and regulations. Federal agencies play a variety of roles in helping to strike this balance, including but not limited to (1) owning and operating certain types of infrastructure, (2) wholesale operation and management of credentialing programs for specific kinds of infrastructure, (3) partial operation and management of credentialing programs, and (4) providing regulations and guidance to help owners and operators implement effective access control. For example, DHS's Transportation Security Administration (TSA) manages the entire Transportation Worker Identification Credential (TWIC) qualification process including enrollment, background checks, and credential

[10] DHS, Screening Coordination Office, *Credentialing Framework Initiative* (Washington, D.C.: July 2008).

[11] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

issuance.[12] However, for the Secure Identification Display Area (SIDA) badge, which facilitates access at airports, and is managed in part by TSA, airport operators use TSA's background check information to ultimately make final decisions about airport access and badge issuance. Similarly, NRC issues regulations related to access control requirements, which are to be implemented by commercial nuclear power plants, and DOD owns and operates U.S. military installations and facilities and uses the Common Access Card (CAC) as one method to facilitate access to semi-restricted areas within the installations.

Workers who need access to multiple types of critical infrastructure to realize their livelihoods—such as truck drivers and carpenters—often encounter different access control efforts. For example, carpenters and contractors working at seaports and airports may require both a TWIC credential for the seaports and SIDA badges for each specific airport. Similarly, industries that work across different critical infrastructure sectors may encounter multiple federal access control efforts. For example, a company producing or storing regulated chemicals on both land and at seaports may encounter different access control efforts depending on the location of the facility.

See Table 1 for a list of selected federally-administered critical infrastructure access control efforts and a brief description of each effort.

[12] The TWIC facilitates unescorted access for maritime workers to secure areas of facilities and vessels regulated under the Maritime Transportation Security Act of 2002. Pub. L. No. 107-295,116 Stat. 2064.

Table 1: Selected Federally-Administered Critical Infrastructure Access Control Efforts

Name of Effort	Sponsoring Agency	Description of Effort
Transportation Worker Identification Credential (TWIC)	Department of Homeland Security (DHS), Transportation Security Administration (TSA), United States Coast Guard	TWIC is designed to protect maritime transportation facilities from terrorism or security threats; the TWIC credential, issued by TSA nationwide, is used by individuals seeking unescorted access to maritime facilities as evidence of an approved security threat assessment.
Hazardous Materials Endorsement (HME)	DHS, TSA	HME is an endorsement a state adds to its issued commercial driver's license that allows endorsed drivers to transport hazardous materials placarded under the Department of Transportation's hazardous materials regulations. TSA performs security threat assessments on applicants seeking an HME through their states' licensing bureaus or departments.
Secure Identification Display Area (SIDA)	DHS, TSA	SIDA is an airport-issued credential designed to leverage TSA background check information by screening individuals requiring unescorted access through designated areas of airport facilities.
Chemical Facility Anti-Terrorism Standards (CFATS)	DHS, National Protection and Programs Directorate	CFATS is designed to identify and regulate high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with the chemicals they possess. Within CFATS, the Personnel Surety Program requires the vetting of facility personnel and unescorted visitors who have, or are seeking access to, restricted areas and critical assets at high-risk chemical facilities.
Commercial Nuclear Power Plant Regulations (Nuclear)	Nuclear Regulatory Commission (NRC)	NRC regulations are designed to require that each commercial nuclear power plant licensee establish, implement, and maintain an access authorization program, including the provision of unescorted access, in accordance with NRC regulations in order to protect against acts of radiological sabotage.
Common Access Card (CAC)	Department of Defense (DOD)	The DOD CAC is primarily a benefits eligibility card, but also serves as the standard identification for DOD military and civilian employees, and eligible contractor personnel used to facilitate physical access to DOD installations. Individuals requiring a CAC must be investigated and adjudicated in accordance with DOD policy.

Source: GAO analysis of DHS, NRC, and DOD access control information. | GAO-17-182

Selected Federal Access Control Efforts have Similar Processes, but Three Key Factors Had an Impact on Stakeholders

Access Control Efforts Follow Similar Processes, but Specific Characteristics of the Efforts Vary

While the six selected federally administered access control efforts we reviewed had varying purposes, standards, or agency responsibilities, they generally included the following process components or phases of DHS's credentialing lifecycle as depicted in Figure 1.

Figure 1: Department of Homeland Security's Credentialing Lifecycle Phases

Registration and enrollment

Occurs when an individual first requests a credential; includes initial collection of biographic data as well as other documentation, such as address and phone number.

Background check

Determination of an individual's eligibility for a requested license, privilege, or status. It includes checking against government and/or commercial databases to confirm identity, identifying relevant derogatory information (such as terrorism information or criminal history), resolution of any derogatory information, and/or confirming the validity of presented documentation, nationality, or immigration status.

Issuance

Personalization of a credential that serves as a mechanism to identify individuals that have been granted a license or privilege. The output of this process may include a physical card or endorsement.

Verification

The actual presentation of the credential by the holder, or use by the decision maker to verify the license, privilege, or status and the identity of the bearer. It includes making a determination that the credential presented is authentic, that the individual presenting the document is the one to whom it was issued or granted, and the license, privilege or status is valid.

Expiration/revocation

Efforts taken to terminate a valid license, privilege, or status and the associated credential based on new information or expiration. Additionally, it includes any provisions a program may take to preclude use of or to exercise the prior license, privilege, or status, and actions taken to recover the expired or revoked credential.

Redress/waiver

Procedures to grant a benefit after (1) determining that initial disqualifying information was not correct (redress) or (2) upon presentation of evidence that the disqualifying factors do not represent a threat warranting denial (waiver).

Source: GAO summary of DHS Credentialing Lifecycle Phases. | GAO-17-182

Although the six efforts we reviewed generally follow similar processes, certain characteristics within these efforts can vary. For instance, we found that roles and responsibilities of the federal administrators and the operator stakeholders in credentialing varied. As an example, TSA is responsible for implementing the entire TWIC credentialing process including enrollment and background checks, while maritime port facility operators—public port authority or privately operated facilities—are responsible for physically verifying the credentials that TSA has issued at ports. In contrast, under the SIDA program, TSA and airport operators each have certain responsibilities for several elements of the credentialing process, including the criminal history record check.

Table 2 summarizes the credentialing processes along with the roles and responsibilities of government and private entities for the six selected efforts we reviewed. Appendix I provides more detailed and specific information about each of the six selected efforts we reviewed.

Table 2: Summary Comparison of Roles and Responsibilities for Selected Access Control Efforts

	ACCESS CONTROL EFFORT					
LIFE-CYCLE PHASE	**Transportation Worker Identification Credential (TWIC)**	**Hazardous Materials Endorsement (HME)**	**Secure Identification Display Area (SIDA)**	**Chemical Facility Anti-Terrorism Standards (CFATS)**	**Commercial Nuclear Power Plant Regulations (NRC)[a]**	**Common Access Card (CAC)**
Registration/ Enrollment	Applicant provides biographic and biometric information at an enrollment center	Applicant provides biographic and biometric information at an enrollment center or to state licensing agency	Applicant provides biographic and biometric information to airport operator, who transfers it to aviation channeling vendor. Vendor ensures that the information is properly formatted and complete before relaying the information to (Transportation Security Administration (TSA) for vetting	Affected individual provides information to chemical facility, which forwards it to the organization that will conduct the vetting	Applicant provides biometric and biographic information to nuclear facility operators that collect and process their applications either directly or with the use of contractors or vendors	Applicant enters biographic information into electronic questionnaire for investigative processing

Vetting/Background Check	TSA vets, adjudicates and makes final determination of eligibility	TSA vets, adjudicates and provides determination of eligibility to state licensing agency and applicant	TSA vets and adjudicates terrorist and immigration checks and provides results of criminal history check to airport operator. Airport operator adjudicates criminal history and makes determination of eligibility.	Facility conducts background check, except for terrorist check. Facility has four options to perform or verify terrorist check: (1) submit information to the Department of Homeland Security (DHS) for vetting; (2) use vetting conducted under a DHS program; (3) use electronic verification of a TWIC; or (4) use visual verification of a document or credential issued by a federal screening program.	Operator sends applicant information to Federal Bureau of Investigation to review criminal history. Military and credit history are also reviewed along with citizenship verification. Nuclear facility operator makes the final determination of eligibility.	Background investigation is conducted by Office of Personnel Management
Issuance	TSA	State licensing agency	Airport badging office	No credential is issued	Nuclear facility operator	Department of Defense (DOD)
Verification and Use	Maritime facility operator	Employers	Airport operator	Chemical facility operator	Nuclear facility operator	DOD facility security
Expiration	5 years	Up to 5 years, depending on individual state issuance policies	Maximum of 2 years	Varies	Varies	Up to 3 years, depending on employment status with DOD
Redress/Waiver	Appeal within TSA, to Administrative Law Judge, and judicial review waiver process	Appeal within TSA, to Administrative Law Judge, and judicial review waiver process	Appeal within TSA, to Administrative Law Judge, and judicial review No waiver process	Operator No waiver process	Operator No waiver process	3-member board convened by DOD component (for both Redress and Waiver)

Source: GAO analysis of DHS, NRC, and DOD questionnaire responses. | GAO-17-182

[a]NRC regulations listed here apply to commercial nuclear power plants.

Access Control Efforts Have Different Impacts on Stakeholders Due to Varying Interests

As previously mentioned, federally-administered access control efforts generally involve two groups of stakeholders: users and operators. Users are individuals who require access to critical infrastructure as an essential function of their job. Users we interviewed that require access to multiple types of critical infrastructure said they recognize the need for security, but are interested in streamlined access control efforts to facilitate legitimate access in a manner that minimizes the related time and costs they incur. They also told us they desire the maximum possible uniformity across standards for background investigation and disqualifying offenses to enhance predictability. Operators are individuals or groups who own or are responsible for managing facilities, such as airports, seaports, and chemical facilities, which may be privately owned, but can also include other government-owned facilities such as military installations. Operators, we spoke with, who are responsible for providing security for critical infrastructure, said they need to maintain control over who enters their facilities so they can manage their accepted level of risk along with the associated costs. Operators said they prefer to retain maximum decision-making authority for granting access as well as the type of credential they use to verify proper vetting.

Based on our interviews with stakeholder groups and associations, the issues mentioned that had an impact on users and operators included (1) operators may add access requirements to vetting and background checks already conducted for federally administered programs; (2) credentials that cannot be used within and across critical infrastructure sectors; and (3) enrollment information that has to be entered multiple times for the same user for similar purposes. It is important to note that although these issues can present challenges for various users and operators, they do not necessarily reflect a deficiency on the part of any specific access control effort or stakeholder group. For the most part, these six selected efforts were created separately in response to different needs, are largely governed by different laws and regulations, and were not necessarily designed to work together.

Facility Operators May Consider Additional Requirements in Making Final Access Decisions

User groups we interviewed expressed a desire to be able to predict denial of access based on clear and standardized requirements; while operator groups described the need for some variability in requirements across sites, so they can manage their context-specific risks. Part of the eligibility vetting process for all the six selected access control efforts we reviewed includes determining if an applicant is on the known or suspected terrorist list or has a criminal history with certain disqualifying offenses that warrant denial of the access. Specific disqualifying offenses can vary across these federal efforts because of differences in the statutes that established the federal efforts.[13] This variability can create some level of complexity for the users of multiple federally-administered efforts, which is compounded when individual on-site critical infrastructure operators impose additional requirements. For example, according to association members representing carpenters, the lack of consistency around whether individuals can qualify for access has led to difficulties aligning staff with critical project tasks. As a result, the time associated with identifying disqualifying offenses can lead to challenges with meeting scheduled project timelines and budgets.

For all six selected federal access control efforts we reviewed, regardless of the way the access effort was structured (whether the infrastructure is government or privately owned and whether an effort is wholly managed by a federal agency or guided by regulation), we found that on-site operators can make the final decision about who can enter their facilities. During our interviews with users and operators we found that on-site operators across multiple infrastructure types have considered additional disqualifying offenses beyond federal baseline requirements. For example with SIDA, CFATS, and commercial nuclear power plants that are regulated under NRC the individual operator examines the individual's criminal background information and makes his or her own determination regarding access based on their perception of acceptable risk.

In addition, we found that site-specific decision making was taking place under federal efforts for which the government was the sole vetting authority, such as TWIC. For example, port authority representatives told us that ports often perform site-specific background checks even for those individuals with an issued TWIC. Port authority representatives provided two key reasons for conducting their own site-specific background checks on top of the federal government's process: (1) the ability to view an individual's comprehensive and recent criminal history and (2) the ability to consider factors that may not be covered in TWIC's list of disqualifying offenses. Some operator groups that we spoke with noted that the disqualifying offenses covered by programs like TWIC, which is designed to limit terrorism risk, do not cover the full range of safety and security concerns that are ultimately their responsibility to control. For example, a representative from the American Association of

[13] For example, the disqualifying offenses and look-back periods for TWIC are governed by 49 U.S.C. § 70105 and 49 C.F.R. § 1572.103 and for SIDA by 49 U.S.C. § 44936 and 49 C.F.R. § 1542.209. The HME effort adopted the same disqualifying offenses as were prescribed for TWIC. 49 C.F.R. § 1572.103.

Airport Executives told us that airports have the discretion to consider requirements beyond federal regulations, which can be used to disqualify applicants for a SIDA. These additional requirements may reside in state or local ordinance, and can vary from airport to airport. Consequently, some operators perform additional vetting on site, which allows them to align vetting policies and procedures with their accepted types and level of risk.

Even when the federal government has sole vetting authority, facility operators and military installation commanders can choose to add additional vetting procedures to ensure they are managing their facilities based on their own accepted level of risk. For example, in 2009, DOD issued a policy directive to accept, among others, the TWIC and the CAC as identification documents authorized to facilitate physical access to installations.[14] However, according to DOD headquarters officials, the military services maintained that the TWIC was not intended to be used for access to military installations, and consequently this policy has not been implemented uniformly across DOD. For example, truck drivers holding TWIC cards and serving military installations have been at times required to undergo additional background and security checks. According to trucking industry representatives, inconsistency across DOD installations is a source of concern as they do not know what might be required of drivers who are trying to gain access. In addition, delays in gaining access to installations can result in increased costs for the truck drivers, and potentially create cascading delays for their subsequent deliveries. Installation commanders have been given the authority to supplement the DOD procedures and process for accessing their installation to help ensure appropriate response to risk with real-time information and decision making. Consequently, the requirements for access can vary by installation.[15] A TSA official also noted that certain sex offenders may be able to get a TWIC, depending on the offense and when the individual was convicted or released from incarceration. The TSA official stated that this is because sexual offenses are not permanently disqualifying under the TWIC statute and may not point to a

[14] Department of Defense, Under Secretary of Defense (Intelligence), *Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control* (Washington, D.C.: Dec. 8, 2009).

[15] On December 23, 2016, the *National Defense Authorization Act for Fiscal Year 2017* was enacted and requires DOD to exempt TWIC-carrying transportation workers with a DOD security clearance from further vetting when seeking unescorted access at DOD facilities. Pub. L. No. 114-328, § 1050(b), 130 Stat. 2000 (2016).

terrorism or security risk of a regulated maritime facility; however, a military commander may not want to allow that individual onto his or her installation where families with young children are housed and so may consider such offenses disqualifying.

Credentials Generally Cannot be Used Within or Across Critical Infrastructure Sectors

User groups we interviewed generally expressed a desire for reciprocity across federally-administered access control efforts, in particular when such efforts have or appear to have the same or similar underlying vetting processes and associated risks. Operators, on the other hand, had mixed perspectives on this issue. While some operators emphasized finding solutions to enhance access control reciprocity, others cited barriers to or challenges with a more uniform approach.

Among the six selected access control efforts we reviewed, we found limited mechanisms to use one credential for access to similar facilities within and across sectors (i.e., reciprocity). Two examples of reciprocity are DOD's CAC,[16] which generally allows access into the semi-restricted areas of most military installations, and the CFATS Personnel Surety Program, which allows regulated high-risk chemical facilities to accept previously-issued TWICs to grant access if they are electronically verified, or other credentials issued through a federally administered screening program, if they are visually verified, and if the screening program periodically vets enrolled individuals against the Terrorist Screening Database.[17] Across the chemical sector, chemical facility access is facilitated by two different access control efforts depending on where the chemical facility is located—land-based facilities are governed by CFATS and maritime-based facilities are governed by TWIC. Officials from NPPD, the DHS component that administers CFATS, stated that NPPD explored allowing land-based chemical facility users to enroll in the TWIC

[16] DOD security policy requires that DOD civilians, military, and contractor personnel use the CAC for access into the semi-restricted areas of most military installations, as the background investigations required for these cards to be issued and the adjudication criteria of derogatory information are standard across the department.

[17] According to the CFATS Personnel Surety Program, chemical facility operators are allowed two other options when performing vetting for terrorist ties: 1) providing information directly to the CFATS program office for vetting; or 2) use vetting conducted under a DHS program; a facility may also propose to the department other approaches to completing the terrorist ties vetting, which the department may consider.

program, but DHS has interpreted the Maritime Transportation Security Act of 2002 to provide limited authority to do so. However, individuals in the field of transportation who are eligible for a TWIC may apply for and receive that credential to satisfy the CFATS requirement. NPPD officials stated that facilities may also use screening results from other agencies, such as the Bureau of Alcohol, Tobacco, Firearms, and Explosives, as long as the vetting process includes checking against the Terrorist Screening Database.

Biographic Information is Collected Multiple Times across Selected Efforts

The user stakeholders we interviewed expressed a desire to be able to enter their biographic information once during the registration and enrollment phase, and have that information reused for other access control efforts, and where possible, for background check processing. Some operator groups we interviewed indicated that it was costly and inefficient for operators and users to enter biographic data multiple times. However, federal administrators are limited in their ability to share biographic information across screening efforts because of information technology, and privacy considerations. Among the six access control efforts we reviewed, there are some mechanisms to reuse biographic information; however, there are no set requirements to do so. For example, operators may collect complete biographic information each time a user applies for a SIDA badge for an airport facility. A user group said that it would like to be able to reuse their biographic information for airports, but TSA officials we interviewed stated that any proposed solution to reuse biographic information would be affected by privacy considerations. Under federal law, personal information collected and maintained by an agency for a particular effort may not be disclosed to another agency, with certain exceptions.[18]

In contrast, within NRC's regulated commercial nuclear power plants, operators use the Personnel Access Database System (PADS) in cooperation with NRC that allows users to provide biographic information once to access multiple facilities because potential employees sign a

[18] 5 U.S.C. § 552a(b) (outlining certain exceptions to this prohibition, such as disclosure to another agency for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought).

release of information form to use the system. Users and operators agreed that they benefited from the ease of PADS because they do not have to submit biographic information for each facility. They told us that PADS allows for employee data to be shared across NRC nuclear power plant facilities in part because it is an industry-operated system that is not constrained by federal privacy requirements that would apply to federal systems.

DHS's Critical Infrastructure Partnership Structures Provide Opportunities to Harmonize Access Control Efforts

DHS Uses Partnership Structures for Critical Infrastructure Protection

DHS has established roles and responsibilities for supporting collaboration efforts among key stakeholders across critical infrastructure sectors. The department also uses partnership structures to enhance information sharing efforts aimed at strengthening critical infrastructure security. According to Presidential Policy Directive/PPD-21 (PPD-21), DHS is responsible for coordinating the overall federal effort to promote the security and resilience of the nation's critical infrastructure, provide strategic guidance, and promote a national unity of effort, among other responsibilities.[19] Within DHS, NPPD's Office of Infrastructure Protection (IP) leads the coordinated national effort to mitigate risk to the nation's critical infrastructure and is responsible for working with public and private sector critical infrastructure partners to enhance security efforts. Using a partnership approach, NPPD IP's Sector Outreach and Programs Division works with owners and operators of the nation's critical infrastructure to develop, facilitate, and sustain strategic relationships and information sharing efforts, including the sharing of best practices. NPPD IP also oversees and supports various partnership councils intended to protect and provide essential functions to enhance response efforts.

[19] Presidential Policy Directive 21/PPD-21—*Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

As reported in the National Infrastructure Protection Plan (NIPP), DHS has created partnership structures to collaborate and engage federal and nonfederal stakeholders in critical infrastructure discussions and to enhance critical infrastructure resilience efforts.[20] These voluntary partnership structures provide forums for critical infrastructure stakeholders—federal, state, local, tribal, territorial, and private sector officials—to come together, exchange ideas, and leverage resources. The Critical Infrastructure Partnership Advisory Council (CIPAC) serves as a forum among critical infrastructure stakeholders to facilitate interaction and coordination of critical infrastructure activities, including planning, coordinating, and exchanging information on cross-sector issues and implementing security and resilience program initiatives. CIPAC membership consists of representatives from the Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC)—federal, state, and local agency officials and private owners and operators, respectively—who work together to coordinate strategies, activities, and policies across governmental entities within each of the 16 critical infrastructure sectors.

The NIPP also establishes voluntary cross-sector councils to develop national priorities related to strengthening critical infrastructure security.[21] Specifically, the Critical Infrastructure Cross-Sector Council provides a forum for SCCs to address cross-sector issues and interdependencies. This council’s activities primarily focus on identifying and disseminating critical infrastructure security and resilience best practices across sectors, and identifying areas where cross-sector collaboration could advance national priorities. Additional cross-sector councils representing state, local, tribal, and territorial partners serve as forums for members to (1) facilitate enhanced communication and coordination across sectors, (2) evaluate and promote implementation of risk-informed critical security and resilience programs, and (3) promote resilience activities in the public and private sectors, mainly through awareness, education, and mentorship on a wide variety of subjects, among other activities. Within NPPD, the Interagency Security Committee (ISC) serves as a forum for chief security officers and other federal agency officials to develop federal security standards and policies to enhance physical security of non-DOD federal

[20] DHS, *National Infrastructure Protection Plan 2013, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[21] DHS, *National Infrastructure Protection Plan 2013, Partnering for Critical Infrastructure Security and Resilience. Appendix A. The National Partnership Structure* (Washington, D.C.: December 2013).

facilities and engage with industry stakeholders to advance best practices. Collectively, these voluntary DHS partnership structures are designed to provide federal agencies a better understanding of the risks associated with critical infrastructure security and an enhanced awareness to make informed decisions about critical infrastructure priorities.

Partnership Structures Provide Opportunities for Harmonization of Access Control Efforts across Critical Infrastructure Sectors

According to NPPD senior officials, DHS voluntary partnership structures exist to discuss a variety of issues that have an impact on critical infrastructure security, but DHS has not used these structures to identify opportunities to harmonize regulated screening and credentialing efforts. The issues discussed earlier in this report about users' and operators' experiences across different access control efforts illustrate that there are administrative burden and costs both within and outside of government when the efforts are inconsistent or their administration appears to be less efficient. However, those findings also highlight that there are few, if any, obvious solutions, as many of the issues involve tradeoffs across competing needs of different stakeholder groups and ongoing consideration of the appropriate balance to manage risk without unnecessarily impeding business and operations. In that regard, NPPD officials stated there are challenges, and developing a one-size fits all approach to harmonizing credentialing procedures is not a feasible solution because of the complexities within and across critical infrastructure sectors. Nonetheless, they acknowledged that finding opportunities to harmonize efforts is a worthwhile goal to pursue.

Guidance from DHS partnership structures and our best practices call for entities to identify and share best practices and to collaborate by seeking means to address needs by leveraging resources and establishing compatible policies, procedures, and practices. Specifically, the CIPAC charter document, calls for CIPAC to facilitate interaction among federal government, private sector, and state, local, territorial, and tribal entities to conduct deliberations and form consensus positions to assist the federal government in engaging in implementing security and resilience program initiatives, including conducting operational activities related to critical infrastructure security, sharing threat, vulnerability and risk information, and best practices with one another. Similarly, our work on enhancing collaboration across organizational boundaries calls for entities to, among other things, (1) identify and address needs by leveraging resources and (2) establish compatible policies, procedures, and other means to operate across agency boundaries.[22]

Given NPPD IP's role as the DHS component responsible for leading the national effort to strengthen the security and resilience of the nation's critical infrastructure, DHS is well positioned to facilitate collaboration across stakeholder groups—users, operators, and federal administrators—to identify opportunities to harmonize access control efforts across critical infrastructure sectors. According to NPPD officials, the CIPAC partnership structure would serve as an appropriate forum for critical infrastructure stakeholders to discuss potential harmonization efforts moving forward. However, NPPD IP officials responsible for overseeing CIPAC and ISC stated that their cross-sector partnership structures have engaged in limited efforts to explore harmonization of access control efforts, because harmonization has not been raised as a key issue or urgent concern by its members.

However, NPPD IP officials stated that issues raised when considering the user perspectives alongside the operator perspectives would not necessarily have emerged in these groups, because as of October 2016, none of the existing CIPAC partnership forums would be appropriate for users or user groups—such as contractors, workers, and others seeking access to multiple critical infrastructure facilities—to share their experiences or concerns. As of October 2016, DHS does not have a dedicated partnership structure that allows for users to share their experiences in navigating through federal access control efforts. Additionally, DHS officials stated that users are not specifically included in the NIPP's Sector Partnership Model.

Moreover, NPPD IP officials from the Sector Outreach and Programs Division, who are responsible for coordinating DHS's partnership structures, stated that government and industry stakeholders have begun initial discussions to enhance information sharing efforts, which could include leveraging information across access control efforts. Specifically, NPPD IP officials reported that during a biannual meeting in July 2016, CIPAC members discussed ways to improve information sharing efforts between government and industry stakeholders related to harmonizing

[22] GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

access control efforts. Further, they reported that government and industry stakeholders agreed to create a CIPAC standing committee designed to identify key concerns and engage with members to propose recommendations aimed at enhancing information sharing efforts. Although this effort represents a step towards beginning the discussion of harmonizing access controls efforts, DHS has not fully engaged all relevant stakeholders, specifically users, to explore whether additional opportunities exist to harmonize access control efforts across critical infrastructure sectors. Using existing partnership structures or creating new forums could help DHS more effectively fulfill its role as the facilitator of shared best practices and enhanced collaboration across critical infrastructure partners. In doing so, DHS may be better positioned to identify and implement opportunities to enhance efficiencies within and across related access control efforts.

SCO Has Taken Actions to Harmonize DHS Access Control Efforts, but Has Not Updated Its Goals and Objectives to Support Its Strategic Framework

SCO Goals and Actions to Harmonize DHS Access Control Efforts

A role of SCO, according to DHS Office of Policy officials, is to serve as a department-wide policy advocate for coordination and harmonization of credentialing and screening efforts within DHS. SCO, which is located in the DHS Office of Policy, maintains roughly 30 full-time equivalent staff across different portfolio teams, such as Identity and Credentialing and Watchlisting and Vetting. SCO officials stated that while it is not the sole entity responsible for assessing and harmonizing screening processes across the department, the office provides subject matter expertise and guidance on screening and credentialing policies and practices with the aim of reducing duplicative, stand-alone DHS programs and processes. SCO works with DHS components that are responsible for overseeing screening and credentialing efforts, such as TSA and NPPD, to achieve

DHS's screening and credentialing harmonization objectives.[23] These objectives include identifying and resolving policy issues and program challenges associated with screening and credentialing, supporting department-wide resources that service screening and credentialing efforts, integrating interdependent resources and processes across DHS programs, and representing DHS to external stakeholders.

SCO officials reported that their primary activities fall into three general categories: consultant activities, investment-related decision activities, and working group participatory activities. Specifically, SCO officials stated that they assist DHS components in developing and improving credentialing and screening programs by participating in department-wide budget decisions, and through departmental or component-specific working groups that help guide the development of new programs or the restructuring of existing programs.

According to officials, SCO relies on two foundational policy documents as the overarching strategic framework for promoting harmonization and instructing components on methods for improving access control programs and processes—the 2006 *Credentialing Initiative Report* (CIR) and the 2008 *Credentialing Framework Initiative* (CFI).[24] The CIR identified common problems, challenges, and areas where DHS could improve screening and credentialing programs and processes. Examples of identified problem areas include inconsistent vetting processes for similar programs and the issuance of multiple credentials in cases where one would be sufficient. The report also identified four recommendations for addressing the aforementioned problems. As part of its efforts to address the recommendations outlined in the CIR, SCO published the CFI, an implementation strategy document designed to guide investments and improve the department's ability to meet its mission by improving screening and credentialing processes.

[23] DHS is made up of eight operational components—Customs and Border Protection, the Federal Emergency Management Agency, the Federal Law Enforcement Training Center, United States Immigration and Customs Enforcement, United States Secret Service, TSA, United States Coast Guard, and United States Citizenship and Immigration Service—along with a number of headquarters offices, including, among others, NPPD and the Office of Policy, which houses SCO.

[24] The *Credentialing Initiative Report* (CIR) was published by SCO on December 12, 2006. It states that SCO, through its Credentialing Initiative, will address a number of specific goals of the 9/11 Commission Report, *Homeland Security Presidential Directive/HSPD-11, Comprehensive Terrorist-Related Screening Procedures*, the Rice-Chertoff Joint Vision Initiative, as well as the Secretary of Homeland Security's goals and priorities.

SCO officials stated that they have engaged with DHS components to advance screening and credentialing efficiencies over the past ten years of operation. Through internal annual accomplishment reports and in interviews, SCO provided several examples of activities they have undertaken to advance each of the recommendations outlined in the CIR to advance screening and credentialing efficiencies.

Recommendation 1: Design credentials to support multiple licenses, privileges or status. SCO led a Common Enrollment Coordinating Council (CECC) sub-team, which was tasked to identify opportunities to develop best practices in DHS' screening and credentialing enrollment environment.[25] Of the 18 recommendations produced by the CECC sub-team, three were approved by the Joint Requirements Council, which plans to escalate recommendations to DHS leadership for study and possible implementation.[26]

Recommendation 2: Vetting processes, associated with like uses and like risks, should not be duplicative. SCO partnered with NPPD and TSA to implement the CFATS Personnel Surety Program, which requires that individuals seeking access to restricted areas or critical assets within high-risk chemical facilities are vetted for ties to terrorism. According to SCO and NPPD officials, SCO worked with NPPD to ensure that CFATS vetting standards were aligned with existing DHS vetting efforts to allow the use of screening resources from TSA.

Recommendation 3: Entitlement to a license, privilege, or status should be verified using electronic scanning technology. SCO officials stated they consulted with the U.S. Coast Guard to develop draft regulations pertaining to the

[25] The Common Enrollment Coordinating Council (CECC) supports the Information-Based Screening and Vetting Portfolio Team (IBSV), which is a body comprised of DHS component and headquarters action officers to analyze the potential use of shared resources and infrastructure to gain cross-component efficiencies. The CECC supports the IBSV Portfolio Team in carrying out the coordination and evaluation of all component-driven initiatives pertaining to common enrollment, such as the alignment and standardization of vetting services, biometric collection devices, enrollment center systems, hardware and software.

[26] The Joint Requirement Council is an executive-level body within DHS that provides oversight of departmental requirements generating process, harmonization efforts, and prioritization of funding recommendations.

implementation of electronic card readers at maritime facilities to more effectively validate the authenticity of TWIC cards. [27] SCO officials stated that many maritime facilities are currently validating TWICs using visual inspection, and these regulations are designed to help reduce that practice. As we have previously reported, the reliance on the visual inspection of TWICs is vulnerable to the use of counterfeit credentials to gain access.[28]

Recommendation 4: Establish a preference for ‘enroll once, use many’ environments. SCO officials stated that they consulted with TSA and the U.S. Coast Guard to ensure that certain biographic data elements collected by TSA from maritime workers, as well as the results of TSA’s terrorist screening check for the TWIC program, were available for individuals also applying for a U.S. Coast Guard-sponsored Merchant Mariner Credential (MMC).[29] According to SCO officials, the result of such efforts was partial reciprocity between the TWIC and MMC programs.

SCO Has Not Updated Its Goals and Objectives to Support its Strategic Framework for Department-wide Access Control Harmonization

In its early years, SCO operated under the direction of the strategic policy vision and implementation plans laid out in the 2006 CIR and the 2008 CFI; however, since then, SCO has not updated the goals and objectives outlined in the implantation plans. The 2008 CFI lists a number of structured tasks necessary to implement its recommendations, including the development of a communications timeline for stakeholder engagement and the development and periodic update of CFI implementation goals and objectives. SCO officials stated that the implementation plans are no longer relevant to SCO’s current role in the department. Moreover, in our discussions with SCO officials they

[27] The Coast Guard published its final electronic reader rule: 81 Fed. Reg. 57,652 (Aug. 23, 2016). DHS officials said they plan to review the rule to determine if it will effectively reduce the validation of TWICs using visual inspection.

[28] GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, GAO-11-657 (Washington, D.C.: May 10, 2011).

[29] The Merchant Mariner Credential is a competency-based credential for U.S. mariners issued by the U.S. Coast Guard.

described several opportunities to harmonize screening and credentialing efforts that DHS had yet to achieve, such as the integration of information technology systems. Officials from the DHS Office of Policy, which oversees SCO operations, stated that Office of Policy goals and objectives for SCO come directly from the DHS Office of the Secretary. However, our review of office goals from fiscal years 2015 and 2016 showed that none of the Office of Policy's goals specifically tasked SCO with actionable goals or objectives in support of the strategic policy vision outlined in the CIR and CFI. Additionally, no guidance from the Secretary's office was issued to SCO from 2009 to 2014.

SCO officials stated that their internal planning processes are largely informal rather than a systematic approach to identifying and documenting strategic goals and objectives that could help SCO management pursue the most promising opportunities to support DHS's harmonization efforts and monitor how well its routine activities align with those goals and objectives. *Standards for Internal Control in the Federal Government* calls for agencies to define objectives clearly to meet its mission, strategic plan, goals, and requirements of applicable laws and regulations.[30] Further, the standards call for management to define objectives in specific and measurable terms so they are understood at all levels of the entity. This involves clearly defining what is to be achieved, who is to achieve it, how it will be achieved, and the timeframes for achievement. Without updated goals and objectives, SCO is missing an important management control to help it ensure that it supports the best opportunities for DHS-wide screening and credentialing harmonization.

Conclusions

Balancing the need to secure critical infrastructure while promoting a harmonized screening and credentialing process to access critical infrastructure continues to pose challenges for stakeholders—users and operators—because their interests vary and are not necessarily aligned with each other. DHS is responsible for leading the federal government's effort to protect the nation's critical infrastructure, and has created partnership structures to support stakeholder collaboration. Therefore it is well-positioned to explore whether opportunities exist among all stakeholders, including users, to harmonize screening and credentialing

[30] See GAO-14-704G (Washington, DC: September 2014). Internal control is a process used by management to help an entity achieve its objectives.

processes to provide access in a timely manner. Although DHS does not have a specific partnership structure dedicated for users to share their experiences, DHS's existing partnership structures or new forums could serve as platforms for all critical infrastructure stakeholders to learn from one another and discuss available options to leverage resources. Using new or existing partnership structures to explore whether opportunities exist to harmonize screening and credentialing processes across critical infrastructure sectors could better position DHS to more effectively balance the need to secure critical infrastructure while promoting harmonized screening and credentialing process.

Within DHS's Office of Policy, the Screening Coordination Office (SCO) is responsible for the coordination and harmonization of screening and credentialing efforts department wide. Although SCO issued foundational policy documents in 2006 and 2008 outlining a strategic framework and implementation plans to harmonize DHS access control efforts, since that time SCO has not updated its goals and objectives to identify improvements needed. Goals and objectives in support of SCO's strategic framework would better position it to pursue the highest priorities and best opportunities for DHS-wide screening and credentialing harmonization.

Recommendations for Executive Action

To enhance its ability to fulfill its role as the facilitator of cross-sector collaboration and best-practices sharing, we recommend that the Secretary of Homeland Security direct the Assistant Secretary of Infrastructure Protection, Office of Infrastructure Protection, take the following action:

> Explore with key critical infrastructure partners, whether and what opportunities exist to harmonize federally-administered screening and credentialing access control efforts across critical infrastructure sectors.

To help ensure that SCO uses its time and resources to pursue the most efficient and effective screening and credentialing harmonization goals on behalf of the department, we recommend that the Secretary of Homeland Security direct the Deputy Assistant Secretary for Screening Coordination, Office of Policy, take the following action:

Establish goals and objectives to support its broader strategic framework for harmonization.

Agency Comments and Our Evaluation

We provided a draft of this report for review and comment to DHS, NRC, and DOD for their review and comment. DHS and NRC provided written comments, which are reproduced in Appendix II and III. In their comments, DHS concurred with each recommendation and described actions underway or planned to address them including estimated timeframes for completion. If fully implemented, these actions should address the intent of the recommendations and better position DHS to balance the need to secure critical infrastructure while promoting a harmonized screening and credentialing process to access critical infrastructure. For example, in regards to exploring whether and what opportunities exist to harmonize federally-administered screening and credentialing access control efforts across critical infrastructure sectors, DHS noted that they are working to harmonize access control efforts across critical infrastructure as much as practical and remain committed to working towards that end with interagency partners. Specific actions identified to be completed around April 2017 include considering drafting a plan that will include an analysis of how to further explore opportunities to harmonize federally-administered screening and credentialing access control efforts across critical infrastructure sectors. More specifically, the Interagency Security Committee will request that its Steering Subcommittee discuss potential avenues for addressing any gaps and areas of further collaboration related to screening and credentialing access control efforts of federal facilities.

In regards to establishing goals and objectives to support the Screening Coordination Office's (SCO) broader strategic framework for harmonization, DHS identified actions to direct SCO to establish updated goals and objectives to support the broader strategic framework for more efficient and effective vetting. SCO will provide their goals and objectives to DHS components once finalized to be completed by June 2017.

DHS and DOD also provided technical comments, which were incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Homeland Security and Defense, and the Chairman of the Nuclear Regulatory Commission. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (404) 679-1875 or CurrieC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made significant contributions to this report are listed in Appendix IV.

Chris P. Currie

Chris P Currie Director, Homeland Security and Justice

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Ron Johnson
Chairman
The Honorable Claire C. McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Thad Cochran
Chairman
The Honorable Richard Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable John Hoeven
Chairman
The Honorable Jon Tester
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Michael McCaul
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Kay Granger
Chairwoman
The Honorable Pete Visclosky
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

The Honorable John Carter
Chairman
The Honorable Lucille Roybal-Allard
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

Appendix I: Life Cycle Characteristics for Selected Access Control Efforts

To address the research question related to describing key characteristics of selected federal access control efforts, we distributed a standard set of questions to three federal agencies—Department of Homeland Security (DHS), Nuclear Regulatory Commission (NRC) and the Department of Defense (DOD).[1] Our questions reflected the screening and credentialing life cycle stages reported by DHS's Screening Coordination Office, including Registration and Enrollment, Vetting, Issuance, Expiration and Revocation, Redress, and Waiver.[2] Tables 3 through 8 below summarize the aggregated responses received from the 3 agencies to our questions.

[1] The NRC access control efforts in the table below refer to the regulation of licensed commercial nuclear power plants.

[2] DHS, Screening Coordination Office, *Credentialing Framework Initiative* (Washington, D.C.: July 2008). For the purposes of our questionnaire, we did not include the Verification phase because this process occurs after the access control system has been established.

Table 3: Life Cycle Phase I: Registration and Enrollment

Department	N/A N/A	Department of Homeland Security (DHS)	N/A	N/A	Nuclear Regulatory Commission (NRC)	Department of Defense (DOD)
PROGRAM	TWIC	HME	SIDA	CFATS	Nuclear	CAC
Information Requested						
Data collected on applicant	Name, address, email address if available, date of birth, gender, height, weight, hair color, and eye color, city, state, and country of birth, fingerprints, facial photograph, immigration status and related information, the reason that the applicant requires a TWIC, the name, telephone number, and address of the applicant's current employer(s), if working for the employer requires a TWIC, if a credentialed mariner or applying to become a credentialed mariner, proof of citizenship.	Name, address, email address if available, date of birth, gender, height, weight, hair color, and eye color, city, state, and country of birth, fingerprints, immigration status and related information, the state of application, commercial driver's license number, and type of HME(s) held, name, telephone number, facsimile number, and address of the applicant's current employer(s).	Name, address, badge information, birthplace, citizenship, date of birth, email, employer information, employer name, fingerprint images, gender, phone number, physical features, criminal history record information.	If applicable, name, citizenship information, date of birth. Other data points may be provided on a voluntary basis. Verification of enrollment in TWIC, HME, or other DHS programs.[a]	Name, country of citizenship, criminal history check, current address, date of birth, eye color, fingerprinting, gender, hair color, height, weight, passport or state issued identification, place of birth, social security number.	Name, driver's license, date of birth, family members' names and addresses,and social security number,[b]
Who collects and analyzes data collected?	Third-party vendor collects data, analyzes personal information; TSA analyses data and runs information through databases. TSA adjudicates the criminal history records check, in addition to the terrorism and immigration checks.	Third-party vendor, collects data, analyzes personal information; TSA analyses data and runs information through databases. TSA adjudicates the criminal history records check, in addition to the terrorism and immigration checks.	Third-party vendors collect information and submit to TSA; TSA runs information through databases. Airport operator adjudicates criminal history records check; TSA adjudicates terrorism and immigration checks.	High-risk chemical facilities collect data and analysis of data depends on which option the facility chooses for vetting.	Operators collect and process their applications either directly or with the use of contractors or vendors.	DOD processes a background investigation application form; U.S. Office of Personnel Management (OPM) processes the background investigation.

Per user application fee	$125.25 new applicant $105.25 if TWIC applicant has HME. $60 to replace a card.	$86.50 in agent states.[c] Varies for non-agent states.	Varies depending on the airport as third-party vendor sets the cost.	DHS does not collect fees for CFATS.	Operators do not collect any fees from applicants.	DOD does not collect any fees from applicants.
Transferability of application data	Can transfer criminal history record information from HME; Security threat assessment (STA) results shared for HME applicants licensed in 27 states if applicants decide to apply prior TWIC STA results.	27 states allow for TWIC security threat assessment (STA) results to be applied toward the HME STA.	No transferability of application data.	CFATS allows transferability of TWIC, HME, and other DHS programs.[a]	Applicants may transfer data, such as fingerprints, and operators may rely on application data from other access programs, consistent with the requirements of 10 C.F.R. § 73.56(h)(5); operators may also rely upon the information that other operators have gathered, pursuant to 10 C.F.R. § 73.56(h)(6).	Application data can be transferred across DOD components. Information in OPM's Central Verification System is available to be shared across the federal government.

Legend

CAC:Common Access Card

CFATS:Chemical Facility Anti-Terrorism Standards

HME:Hazardous Materials Endorsement

SIDA:Secure Identification Display Area

TSA:Transportation Security Administration

TWIC:Transportation Worker Identification Credential

Source: GAO analysis of DHS, NRC, and DOD questionnaire responses, and DOD documentation. | GAO-17-182

[a] Other DHS programs include NEXUS, Global Entry, Free and Secure Trade (FAST), or Secure Electronic Network for Travelers Rapid Inspection (SENTRI).

[b] Data elements are used in conducting background investigation.

[c] Agent states are states that have signed on with TSA's contractor to collect enrollment information and perform the security threat assessment.

Table 4: Life Cycle Phase II: Vetting

	Department of Homeland Security (DHS)				Nuclear Regulatory Commission (NRC)	Department of Defense (DOD)
PROGRAM	**TWIC**	**HME**	**SIDA**	**CFATS**	**Nuclear**	**CAC**
Information Requested						

Timeline for Vetting	30 days.	45 days.	45 days.	Varies—depends on which option facility chooses.[a]	Varies—depends on the procedures of the individual operators.	Varies, depending on the type of background investigation required.
What are the disqualifying offenses?	Disqualifying offenses are outlined in 49 C.F.R. § 1572.103; disqualifying offenses include, but are not limited to terrorism, murder, improper transportation of hazardous materials, or a crime involving a transportation security incident.[b]	Disqualifying offenses are outlined in 49 C.F.R. § 1572.103; disqualifying offenses include, but are not limited to terrorism, murder, improper transportation of hazardous materials, or a crime involving a transportation security incident.[b]	Disqualifying offenses are outlined in 49 C.F.R. § 1542.209; such disqualifying offenses include, but are not limited to murder, armed robbery, distribution of, or intent to distribute, a controlled substance, or carrying a firearm or explosive on aircraft.[c]	Varies—depending on chemical facility site-specific plan. Additionally, disqualifying offences for terrorist ties check may vary depending on which option facility chooses to meet terrorist ties check requirements.[a]	Varies—depends on the procedures of the individual operators. NRC regulations require that the licensee's or applicant's reviewing official evaluate the entire criminal history record of an individual who is applying for unescorted access or unescorted access authorization to determine whether the individual has a record of criminal activity that may adversely impact his or her trustworthiness and reliability. 10 C.F.R. § 73.56(d)(7)).	DOD Instruction 5200.46 outlines conditions that may be disqualifying, which include a single serious crime or multiple lesser offenses that put the safety of people at risk or threaten the protection of property or information, dishonest acts, such as theft and accepting bribes, and deceptive or illegal financial practices, such as embezzlement and check fraud.
Are prior background checks considered?	Yes.	Yes, for drivers licensed in 27 states.	No.[d]	Yes—TWIC, HME, and other select federal screening programs, if the facility chooses that option.[e]	Yes—as long as prior background checks are consistent with the program, pursuant to 10 C.F.R. § 73.56(h)(5).	Yes—if the person is still in clearance eligibility, DOD can accept favorable adjudicated investigations to issue a CAC once the applicant is enrolled in the Defense Enrollment Eligibility Reporting System.
Who makes the final determination?	TSA.	TSA.	Airport operator, unless a terrorist- or immigration-related issue, which is determined by TSA.	Operators make all final determinations.	Operators make all final determinations.	DOD component.

What is the cost to the agency of vetting?	Cost is entirely fee funded.	Cost is entirely fee funded.	TSA collects a fee to cover the FBI's costs in performing Criminal History Records Check, which are passed on to the airport badging offices.	DHS incurs the full costs to conduct terrorist database checks using appropriated funds through interagency agreements.	Varies—depends on the procedures of the individual operators.	Administrative, labor,overhead costs incurred by DOD.
What vetting information is shared between federal administrator or operators?	STA results shared for HME applicants licensed in 27 states if applicants decide to apply prior TWIC STA results.	STA results shared for TWIC applicants if applicants decide to apply prior HME STA results.	Vetting information is not shared with other agencies; however, DHS, is considering plans to use internal systems to share information across the department.	DHS can share information collected with other agencies and operators as described in CFATS' System of Records Notice.	All operators use a personnel database system as an electronic means for storing and sharing vetting information across the industry.	Information is stored in OPM's Electronic Questionnaires for Investigative Processing (e-QIP) system and is available per Office of Personnel Management's e-QIP System of Records Notice.

Legend

CAC:Common Access Card

CFATS:Chemical Facility Anti-Terrorism Standards

FBI:Federal Bureau of Investigation

HME:Hazardous Materials Endorsement

SIDA:Secure Identification Display Area

TSA:Transportation Security Administration

TWIC:Transportation Worker Identification Credential

Source: GAO analysis of DHS, NRC, and DOD questionnaire responses, and DOD documentation. | GAO-17-182

[a] CFATS Personnel Surety Program provides four vetting options for facilities to perform or verify terrorist ties check: (1) submit information to DHS for vetting; (2) use vetting conducted under a DHS program; (3) use electronic verification of a TWIC; or (4) use visual verification of a document or credential.

[b] In addition to the permanent disqualifying offenses, the regulation lists other offenses that are interim disqualifying offenses, such that the applicant is disqualified if either the applicant was convicted, or found not guilty by reason of insanity, of one of the interim disqualifying offenses within seven years of the date of the application or the applicant was incarcerated for that crime and released from incarceration within five years of the date of the application.

[c] An individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the listed disqualifying crimes in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.

[d] Airport operators must authorize for unescorted access authority an employee of the federal, state, or local government (including a law enforcement officer) who, as a condition of employment, has been subjected to an employment investigation that includes a criminal records check. Further, airport operators may authorize certain individuals to have unescorted access authority who have undergone a criminal records check through TSA or the Federal Aviation Administration.

[e] Other DHS programs include NEXUS, Global Entry, Free and Secure Trade (FAST), or Secure Electronic Network for Travelers Rapid Inspection (SENTRI).

Table 5: Life Cycle Phase III: Issuance

		Department of Homeland Security (DHS)			Nuclear Regulatory Commission (NRC)	Department of Defense (DOD)
PROGRAM	**TWIC**	**HME**	**SIDA**	**CFATS**	**Nuclear**	**CAC**
Information Requested						
What is issued?	TWIC Card.	State applies HME to commercial driver's license.	Airport badging office issues physical credential.	Nothing—CFATS does not issue a credential.	Each operator grants an unescorted access badge.	CAC.
Who is the issuing agency?	TSA.	State motor vehicle department/division.	Airports' badging offices.	N/A	Individual operators.	DOD.
How is the applicant notified?	Automated phone call, or e-mail, or letter from TSA.	Applicants are mailed a letter and emailed as a courtesy.	The badging office notifies the applicant and issues the credential.	N/A	Licensees are responsible for notifying applicants whether access is granted; however, regulations do not prescribe notification methods.	The sponsoring activity will notify applicant, who then has to schedule an appointment to have the CAC issued.
How does the applicant receive the credential?	US postal service mail or in person pick up.	State is notified and credential becomes part of the applicant's driver's license.	Badging office issues the credential per the airport's procedures.	N/A	Licensees issue badges in person to applicants granted unescorted access.	In person.

Legend

CAC:Common Access Card

CFATS:Chemical Facility Anti-Terrorism Standards

HME:Hazardous Materials Endorsement

SIDA:Secure Identification Display Area

TSA:Transportation Security Administration

TWIC:Transportation Worker Identification Credential

Source: GAO analysis of DHS, NRC, and DOD questionnaire responses, and DOD documentation. | GAO-17-182

Table 6: Life Cycle Phase IV: Expiration and Revocation

	Department of Homeland Security (DHS)				Nuclear Regulatory Commission (NRC)	Department of Defense (DOD)
PROGRAM	**TWIC**	**HME**	**SIDA**	**CFATS**	**Nuclear**	**CAC**
Information Requested						
What is the length of validity for the credential?	5 years.	Up to five years, depending on individual state issuance policies.	Maximum of 2 years—airports can shorten length of time.	N/A	Varies—but NRC requires reinvestigation at least every 3-5 years.	Up to 3 years depending on employment status with DOD.
What information is required to renew the credential?	Applicant must complete entire application process again like a new applicant.	Applicant must complete entire application process again like a new applicant.	Applicant can verify previous information is correct, and the airport can submit a renewal reusing the fingerprints. If biographic information has changed, the airport can submit an update.	N/A	Applicant must complete the entire application process again and operators must comply with the requirements set forth in 10 C.F.R. § 73.56(h)(4)(ii) for update or reinstatement.	Varies—depends on the access needs of the individual.

What are the revocation criteria?	Recurrent vetting looks for hits in the terrorist screening database, and individuals must surrender TWIC if convicted of, wanted, under indictment or complaint, or found not guilty by reason of insanity for a disqualifying criminal offense, adjudicated as lacking mental capacity or committed to a mental health facility; renounces or loses U.S. citizenship or status as a lawful permanent resident; or violates his or her immigration status and/or is ordered removed from the United States.	Recurrent vetting looks for hits in the terrorist screening database and, individuals must surrender HME if convicted of, wanted, under indictment or complaint, or found not guilty by reason of insanity for a disqualifying criminal offense, adjudicated as lacking mental capacity or committed to a mental health facility; renounces or loses U.S. citizenship or status as a lawful permanent resident; or violates his or her immigration status and/or is ordered removed from the United States.	If a change occurs with the applicant's status as a security threat, an investigation is conducted, or if the applicant is convicted or found not guilty by reason of insanity of a disqualifying crime.	N/A—CFATS itself does not set revocation criteria.	NRC has permanent denials for certain violations under 10 C.F.R. part 26. Otherwise, it depends on each operator's procedures.	Federal Investigative Standards guidance on disqualifying and adjudication criteria and DOD instruction 5200.46.
Who determines revocation?	Applicant/case is referred to TSA Office of Law Enforcement/Federal Air Marshal Service.	The TSA Investigations, Referrals and Analysis group or the Law Enforcement Investigations Unit will review cases that fall into these criteria.	Airport Badging Office.	N/A	Operators.	DOD Component or Defense Office of Hearings and Appeals (DOHA).
How is user notified of revocation?	TSA will send written notice to the TWIC holder and apprise them of the redress process available to them.	TSA will send written notice to the user and apprise them of the redress process available to them.	Airport Badging Office.	N/A	Varies—depends on the procedures of the individual operators.	DOD will send letter of denial or revocation to individual and apprise them of the redress process.

How are revocation determinations transmitted to operators?	TSA updates the Canceled Card List daily. All cards that have not reached their expiration date and are canceled, revoked or suspended are on the Canceled Card List, which is available for download by vessel and facility security personnel.	Telephone and/or email to the state motor vehicle department/ division.	Airport sends TSA its revocation message through a third-party vendor.	N/A	Operators update information in the personnel access database to share biographic information with other operators.	Card issuer places the CAC credential on the Certificate Revocation List using the automated Electronic Physical Access control systems.

Legend

CAC:Common Access Card

CFATS:Chemical Facility Anti-Terrorism Standards

HME:Hazardous Materials Endorsement

SIDA:Secure Identification Display Area

TSA:Transportation Security Administration

TWIC:Transportation Worker Identification Credential

Source: GAO analysis of DHS, NRC, and DOD questionnaire responses, and DOD documentation. | GAO-17-182

Table 7: Life Cycle Phase VI: Redress

	Department of Homeland Security (DHS)				Nuclear Regulatory Commission (NRC)	Department of Defense (DOD)
PROGRAM	**TWIC**	**HME**	**SIDA**	**CFATS**	**Nuclear**	**CAC**
Information Requested						
How does an individual apply for redress?	An applicant may appeal a "Preliminary Determination of Ineligibility" (PDI); an applicant may then appeal the final determination to an administrative law judge (ALJ) and the ALJ decision to a TSA Final Decision Maker; applicants may seek judicial review after the Final Determination of Ineligibility or after the determination by the TSA Final Decision Maker.	An applicant may appeal a PDI; an applicant may then appeal the final determination to an ALJ and the ALJ decision to a TSA Final Decision Maker; applicants may seek judicial review after the Final Determination of Ineligibility or after the determination by the TSA Final Decision Maker.	An applicant may appeal the TSA letter explaining its preliminary determination; an applicant may then appeal the final determination to an ALJ and appeal the ALJ decision to a TSA Final Decision Maker; an applicant may seek judicial review of the determination by the TSA Final Decision Maker.	CFATS itself does not set a redress policy; rather, CFATS encourages a chemical facility to include a redress process as part of each operator's site security plan.	The appeal process applicable to nuclear power plant operators is set forth in 10 C.F.R. § 73.56(l); each operator must determine how it will meet the requirement of the redress procedure.	New civilian and contractor applicants who have been denied a CAC may elect to appeal to a three member board convened by the DOD component, composed of not more than one security representative and one human resources representative; contractor employees who have had their CAC revoked may appeal the unfavorable determination to the Defense Office of Hearings and Appeals (DOHA).
Who makes the determination in the redress process?	TSA or Administrative Law Judge or court of jurisdiction.	TSA or Administrative Law Judge or court of jurisdiction.	TSA or Administrative Law Judge or court of jurisdiction.	Depends on the facility's redress process.	Operators.	DOD 3-member board described above or DOHA makes the final determination.
What is the timeframe of the redress process?	60 days from the time of PDI receipt. If an applicant does not respond, the PDI serves as the Final Determination of Ineligibility.	60 days from the time of PDI receipt. If an applicant does not respond, the PDI serves as the Final Determination of Ineligibility.	TSA holds the case in a state of redress for 75 days after the initial denial.	N/A	Varies—depends on the procedures of the individual operators.	30 days—applicant must respond to DOD within 30 calendar days or CAC will be denied/revoked.

Is there interim access during the redress process?	No.	Applicants who are renewing their HMEs and are undergoing the STA process may continue to hold an HME until TSA makes a final determination that their redress material is insufficient or inapplicable.	Yes, user can gain access by being escorted by another SIDA user per the discretion of the airport.	N/A	There are no interim or temporary access benefits pursuant to 10 C.F.R. § 73.56(l).	In certain circumstances.[a]
How is a final determination shared with stakeholders?	Upon completion of a redress determination, TSA sends the applicant a letter advising of approval or denial of the waiver request or appeal.	The state motor vehicle department/division is alerted to the approval or denial.	Final determination is sent to the badging office from TSA via the third-party vendor.	N/A	Operators update information in the personnel database system to share updated results with other operators.	Sponsoring activity must record the final eligibility determination—such as active, revoked, denied—in the Office of Personnel Management Central Verification System.

Legend

CAC:Common Access Card

CFATS:Chemical Facility Anti-Terrorism Standards

HME:Hazardous Materials Endorsement

SIDA:Secure Identification Display Area

TSA:Transportation Security Administration

TWIC:Transportation Worker Identification Credential

Source: GAO analysis of DHS, NRC, and DOD questionnaire responses. | GAO-17-182

[a] An applicant may be issued a CAC on an interim basis, based on a favorable National Agency Check or a Federal Bureau of Investigation National Criminal History Check (fingerprint check). However, if the vetting process supports an unfavorable credentialing determination, the applicant may be able to go through the redress process.

Table 8: Life Cycle Phase VII: Waiver

		Department of Homeland Security (DHS)			Nuclear Regulatory Commission (NRC)	Department of Defense (DOD)
PROGRAM	**TWIC**	**HME**	**SIDA**	**CFATS**	**Nuclear**	**CAC**
Information Requested						
Is there a waiver process?	Yes.	Yes.	No.	CFATS itself does not set a waiver policy.	No.	Yes – essentially the same as Redress process.
On what basis are waivers granted?	TSA may issue a waiver of the criminal offense, immigration, and or mental capacity standards and grant a TWIC if TSA determines that an applicant does not pose a security threat based on a review of information associated with the disqualifying offense/condition.	TSA may issue a waiver of the criminal offense, immigration, and or mental capacity standards and grant approval for an HME if TSA determines that an applicant does not pose a security threat based on a review of information associated with the disqualifying offense/condition.	N/A	N/A	N/A	Among other things, DOD board determines that disqualifying behavior happened so long ago, was minor in nature, or happened under such unusual circumstances that it is unlikely to recur; charges were dismissed or evidence was provided that the person did not commit the offense and details and reasons support his or her innocence.
Who makes the waiver determination?	TSA's Waiver Review Board, or administrative law judge, or TSA Final Decision Maker, or court of jurisdiction if the waiver denial is appealed.	TSA's Waiver Review Board or administrative law judge, or TSA Final Decision Maker, or court of jurisdiction if the waiver denial is appealed.	N/A	N/A	N/A	DOD Component or Defense Office of Hearings and Appeals (DOHA).
How is the waiver determination information shared with stakeholders?	The decision is not shared with other agencies or stakeholders.	The state motor vehicle department/division is alerted to the approval or denial of the waiver.	N/A	N/A	N/A	Sponsoring activity must record the final eligibility determination—such as active, revoked, denied—in the Office of Personnel Management Central Verification System.
What is the timeframe of the waiver process?	TSA has 60 days to review an applicant's waiver application.	TSA has 60 days to review an applicant's waiver application.	N/A	N/A	N/A	30 days.

Legend

CAC:Common Access Card

CFATS:Chemical Facility Anti-Terrorism Standards

HME:Hazardous Materials Endorsement

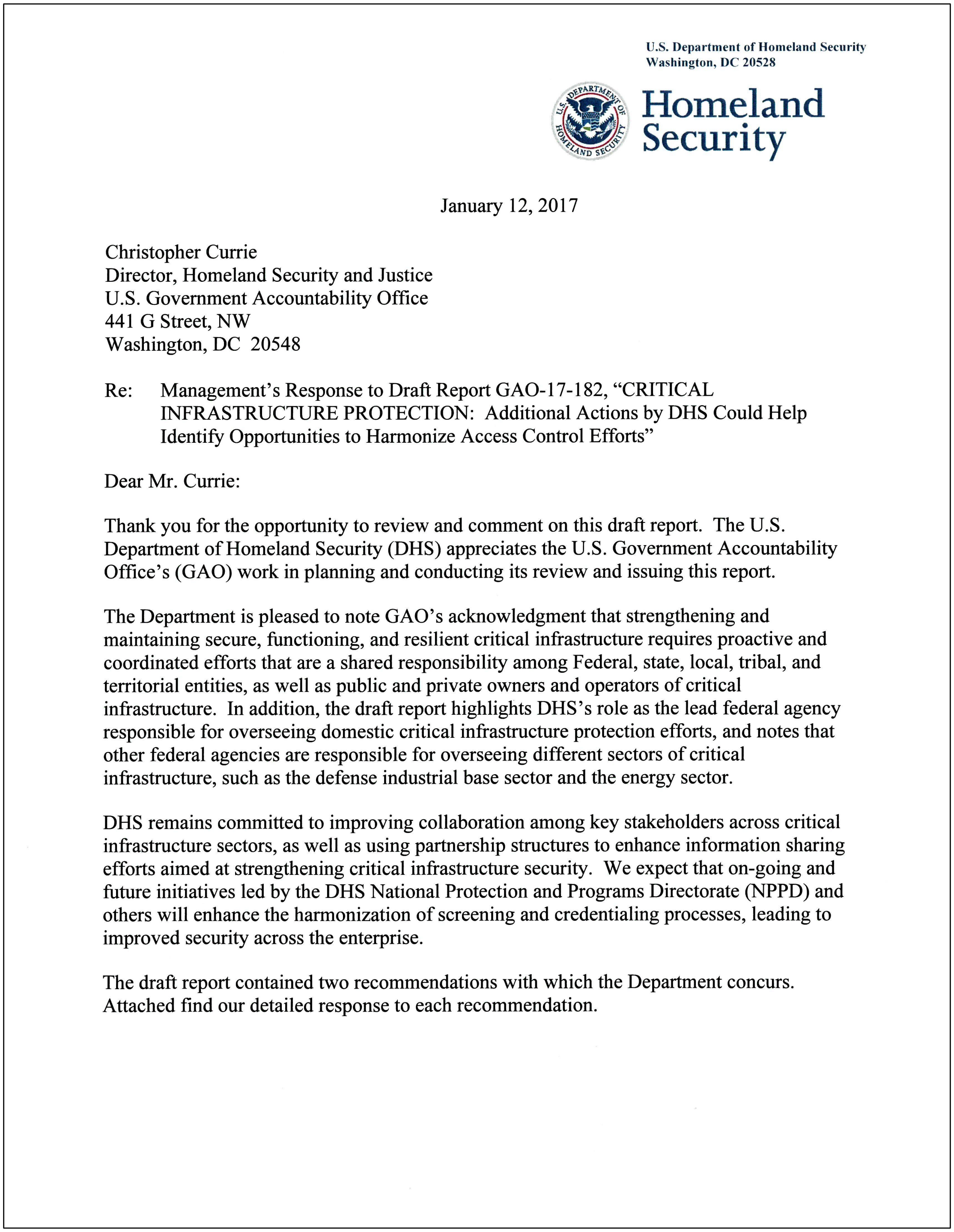
SIDA:Secure Identification Display Area

TSA:Transportation Security Administration

TWIC:Transportation Worker Identification Credential

Source: GAO analysis of DHS, NRC, and DOD questionnaire responses. | GAO-17-182

Appendix II: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

January 12, 2017

Christopher Currie
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management's Response to Draft Report GAO-17-182, "CRITICAL INFRASTRUCTURE PROTECTION: Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts"

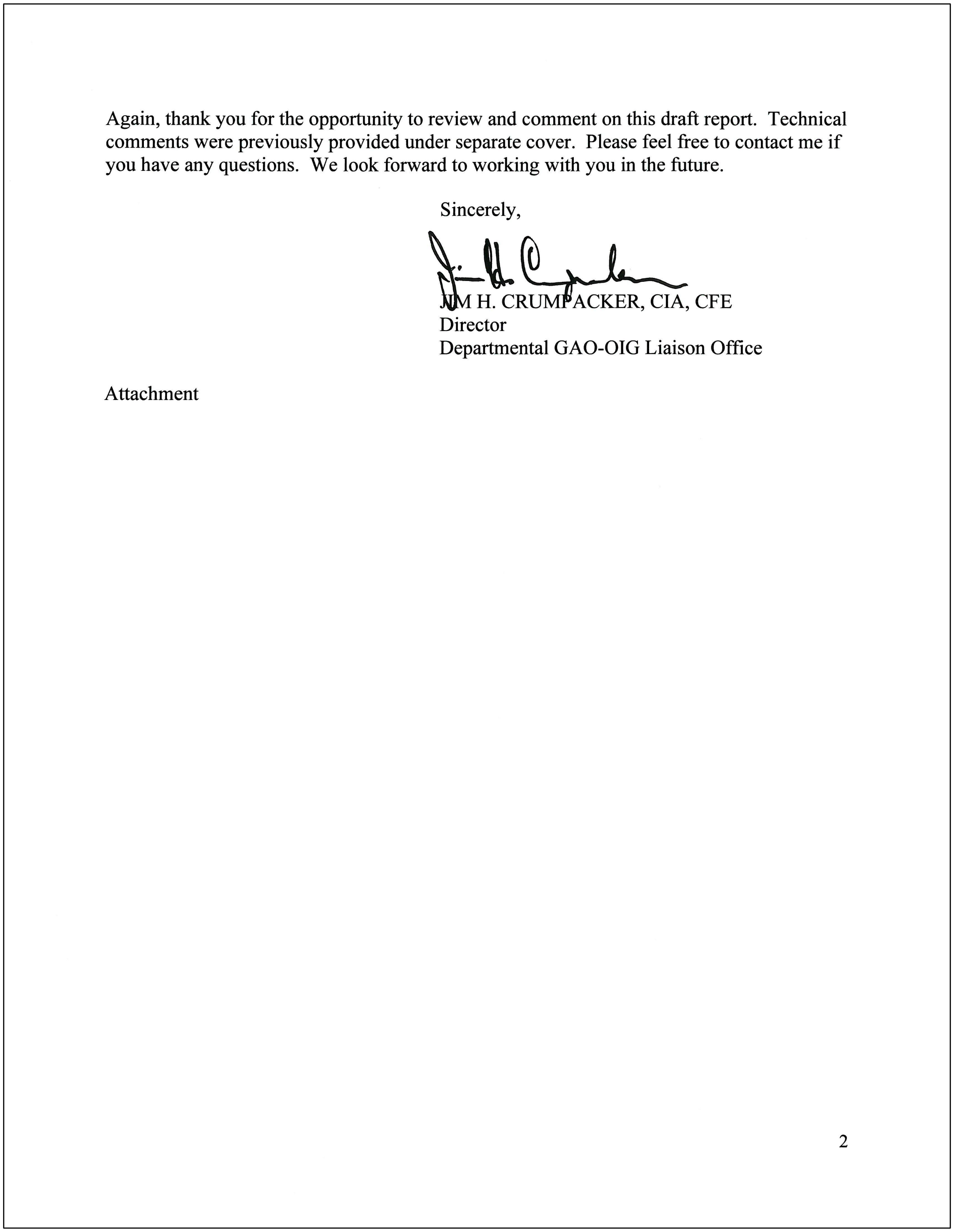
Dear Mr. Currie:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's acknowledgment that strengthening and maintaining secure, functioning, and resilient critical infrastructure requires proactive and coordinated efforts that are a shared responsibility among Federal, state, local, tribal, and territorial entities, as well as public and private owners and operators of critical infrastructure. In addition, the draft report highlights DHS's role as the lead federal agency responsible for overseeing domestic critical infrastructure protection efforts, and notes that other federal agencies are responsible for overseeing different sectors of critical infrastructure, such as the defense industrial base sector and the energy sector.

DHS remains committed to improving collaboration among key stakeholders across critical infrastructure sectors, as well as using partnership structures to enhance information sharing efforts aimed at strengthening critical infrastructure security. We expect that on-going and future initiatives led by the DHS National Protection and Programs Directorate (NPPD) and others will enhance the harmonization of screening and credentialing processes, leading to improved security across the enterprise.

The draft report contained two recommendations with which the Department concurs. Attached find our detailed response to each recommendation.

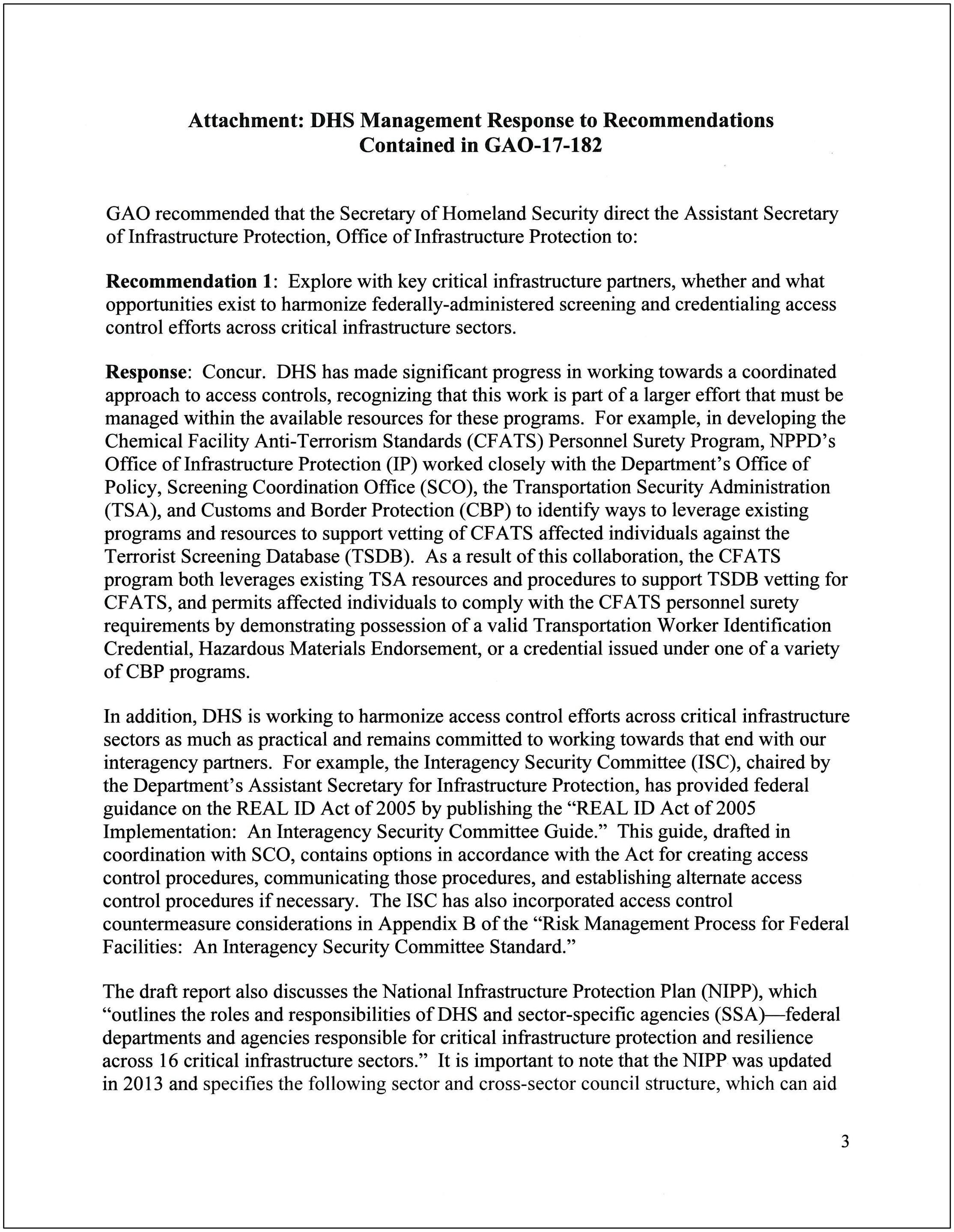


Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment



Attachment: DHS Management Response to Recommendations Contained in GAO-17-182

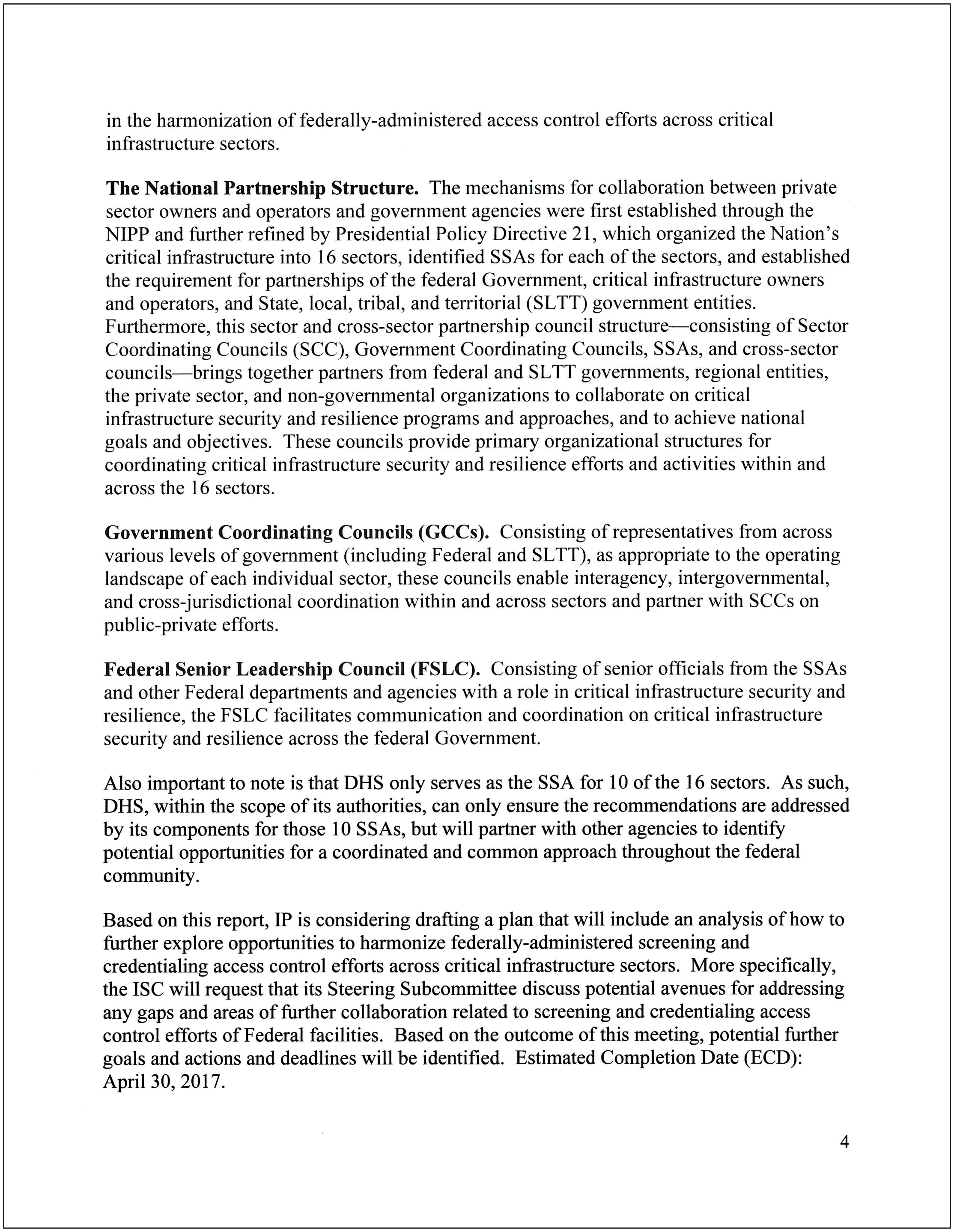
GAO recommended that the Secretary of Homeland Security direct the Assistant Secretary of Infrastructure Protection, Office of Infrastructure Protection to:

Recommendation 1: Explore with key critical infrastructure partners, whether and what opportunities exist to harmonize federally-administered screening and credentialing access control efforts across critical infrastructure sectors.

Response: Concur. DHS has made significant progress in working towards a coordinated approach to access controls, recognizing that this work is part of a larger effort that must be managed within the available resources for these programs. For example, in developing the Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program, NPPD's Office of Infrastructure Protection (IP) worked closely with the Department's Office of Policy, Screening Coordination Office (SCO), the Transportation Security Administration (TSA), and Customs and Border Protection (CBP) to identify ways to leverage existing programs and resources to support vetting of CFATS affected individuals against the Terrorist Screening Database (TSDB). As a result of this collaboration, the CFATS program both leverages existing TSA resources and procedures to support TSDB vetting for CFATS, and permits affected individuals to comply with the CFATS personnel surety requirements by demonstrating possession of a valid Transportation Worker Identification Credential, Hazardous Materials Endorsement, or a credential issued under one of a variety of CBP programs.

In addition, DHS is working to harmonize access control efforts across critical infrastructure sectors as much as practical and remains committed to working towards that end with our interagency partners. For example, the Interagency Security Committee (ISC), chaired by the Department's Assistant Secretary for Infrastructure Protection, has provided federal guidance on the REAL ID Act of 2005 by publishing the "REAL ID Act of 2005 Implementation: An Interagency Security Committee Guide." This guide, drafted in coordination with SCO, contains options in accordance with the Act for creating access control procedures, communicating those procedures, and establishing alternate access control procedures if necessary. The ISC has also incorporated access control countermeasure considerations in Appendix B of the "Risk Management Process for Federal Facilities: An Interagency Security Committee Standard."

The draft report also discusses the National Infrastructure Protection Plan (NIPP), which "outlines the roles and responsibilities of DHS and sector-specific agencies (SSA)—federal departments and agencies responsible for critical infrastructure protection and resilience across 16 critical infrastructure sectors." It is important to note that the NIPP was updated in 2013 and specifies the following sector and cross-sector council structure, which can aid



in the harmonization of federally-administered access control efforts across critical infrastructure sectors.

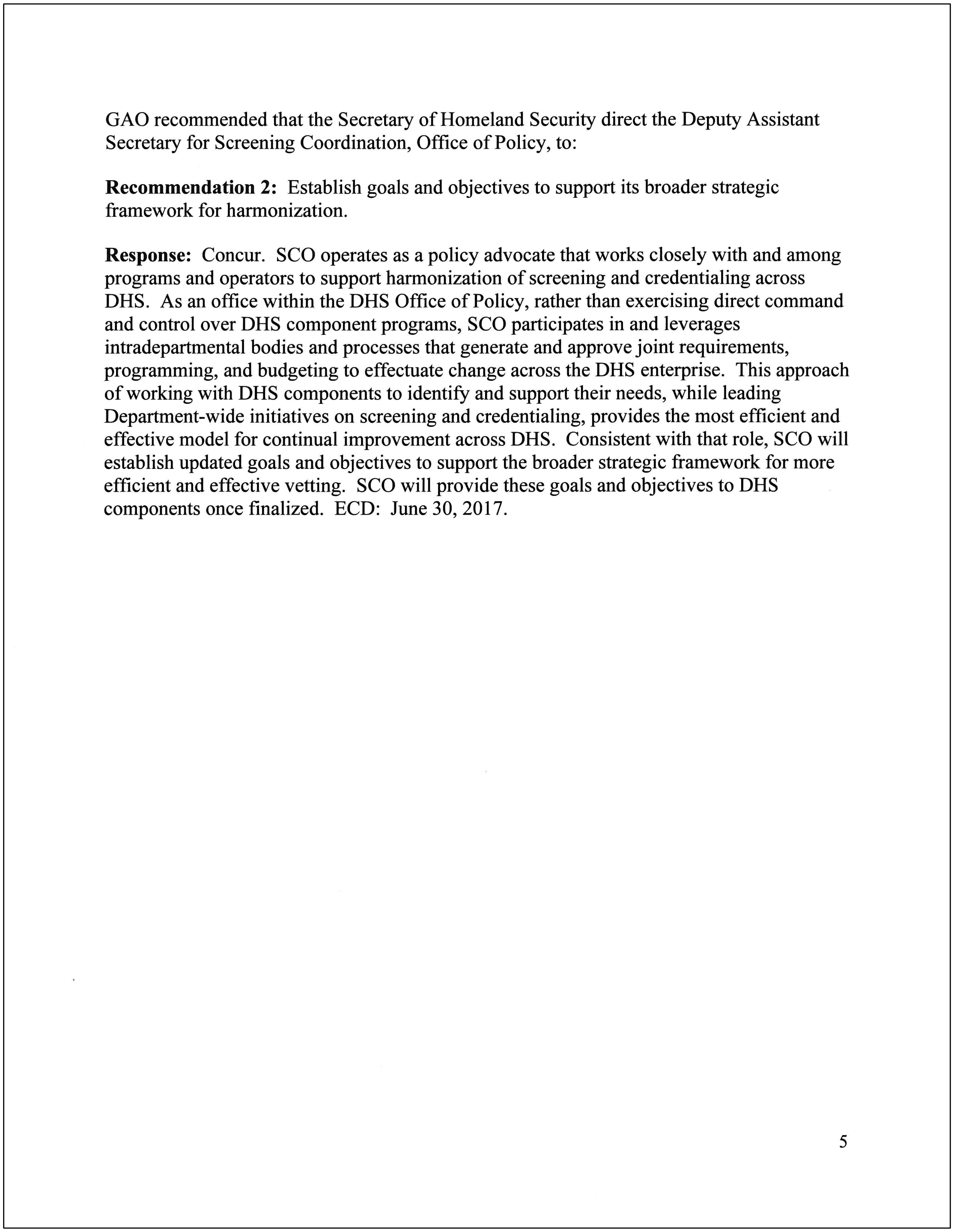
The National Partnership Structure. The mechanisms for collaboration between private sector owners and operators and government agencies were first established through the NIPP and further refined by Presidential Policy Directive 21, which organized the Nation's critical infrastructure into 16 sectors, identified SSAs for each of the sectors, and established the requirement for partnerships of the federal Government, critical infrastructure owners and operators, and State, local, tribal, and territorial (SLTT) government entities. Furthermore, this sector and cross-sector partnership council structure—consisting of Sector Coordinating Councils (SCC), Government Coordinating Councils, SSAs, and cross-sector councils—brings together partners from federal and SLTT governments, regional entities, the private sector, and non-governmental organizations to collaborate on critical infrastructure security and resilience programs and approaches, and to achieve national goals and objectives. These councils provide primary organizational structures for coordinating critical infrastructure security and resilience efforts and activities within and across the 16 sectors.

Government Coordinating Councils (GCCs). Consisting of representatives from across various levels of government (including Federal and SLTT), as appropriate to the operating landscape of each individual sector, these councils enable interagency, intergovernmental, and cross-jurisdictional coordination within and across sectors and partner with SCCs on public-private efforts.

Federal Senior Leadership Council (FSLC). Consisting of senior officials from the SSAs and other Federal departments and agencies with a role in critical infrastructure security and resilience, the FSLC facilitates communication and coordination on critical infrastructure security and resilience across the federal Government.

Also important to note is that DHS only serves as the SSA for 10 of the 16 sectors. As such, DHS, within the scope of its authorities, can only ensure the recommendations are addressed by its components for those 10 SSAs, but will partner with other agencies to identify potential opportunities for a coordinated and common approach throughout the federal community.

Based on this report, IP is considering drafting a plan that will include an analysis of how to further explore opportunities to harmonize federally-administered screening and credentialing access control efforts across critical infrastructure sectors. More specifically, the ISC will request that its Steering Subcommittee discuss potential avenues for addressing any gaps and areas of further collaboration related to screening and credentialing access control efforts of Federal facilities. Based on the outcome of this meeting, potential further goals and actions and deadlines will be identified. Estimated Completion Date (ECD): April 30, 2017.

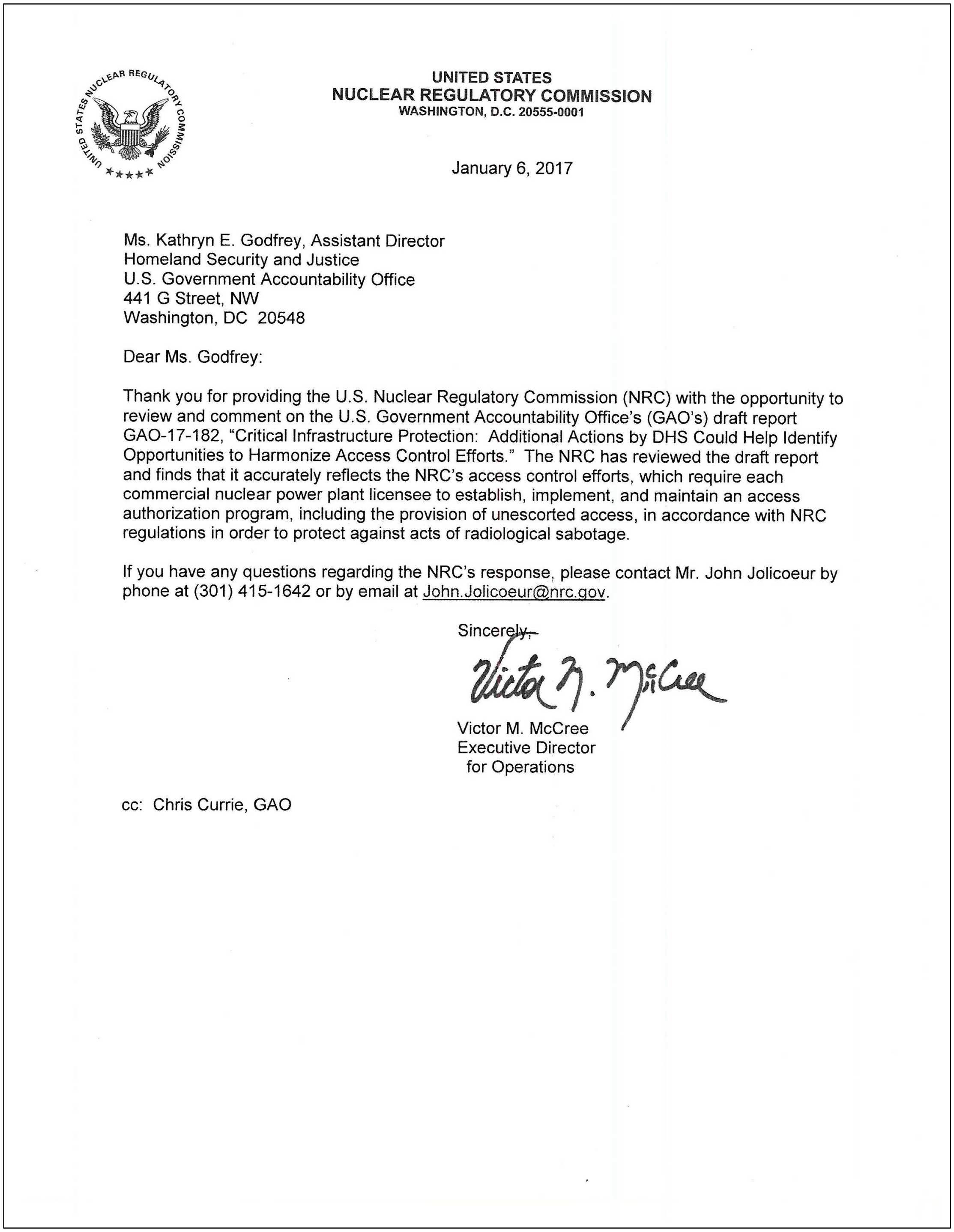


GAO recommended that the Secretary of Homeland Security direct the Deputy Assistant Secretary for Screening Coordination, Office of Policy, to:

Recommendation 2: Establish goals and objectives to support its broader strategic framework for harmonization.

Response: Concur. SCO operates as a policy advocate that works closely with and among programs and operators to support harmonization of screening and credentialing across DHS. As an office within the DHS Office of Policy, rather than exercising direct command and control over DHS component programs, SCO participates in and leverages intradepartmental bodies and processes that generate and approve joint requirements, programming, and budgeting to effectuate change across the DHS enterprise. This approach of working with DHS components to identify and support their needs, while leading Department-wide initiatives on screening and credentialing, provides the most efficient and effective model for continual improvement across DHS. Consistent with that role, SCO will establish updated goals and objectives to support the broader strategic framework for more efficient and effective vetting. SCO will provide these goals and objectives to DHS components once finalized. ECD: June 30, 2017.

Appendix III: Comments from the Nuclear Regulatory Commission



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

January 6, 2017

Ms. Kathryn E. Godfrey, Assistant Director
Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Godfrey:

Thank you for providing the U.S. Nuclear Regulatory Commission (NRC) with the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report GAO-17-182, "Critical Infrastructure Protection: Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts." The NRC has reviewed the draft report and finds that it accurately reflects the NRC's access control efforts, which require each commercial nuclear power plant licensee to establish, implement, and maintain an access authorization program, including the provision of unescorted access, in accordance with NRC regulations in order to protect against acts of radiological sabotage.

If you have any questions regarding the NRC's response, please contact Mr. John Jolicoeur by phone at (301) 415-1642 or by email at John.Jolicoeur@nrc.gov.

Sincerely,

Victor M. McCree

Victor M. McCree
Executive Director
for Operations

cc: Chris Currie, GAO

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Chris Currie, (404) 679-1875 or CurrieC@gao.gov

Staff Acknowledgments

In addition to the contact named above, Kathryn Godfrey (Assistant Director), Amber Edwards (Analyst-in-Charge), Josh Diosomito, Adrian Pavia, Vijay Barnabas, Tracey King, Richard Hung, Lorraine Ettaro, Dominick Dale, Marc Schwartz, and Joseph Kirschbaum made key contributions to this report.

(100547)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548