Privacy Impact Assessment

for the

CISA Gateway

DHS Reference No. DHS/CISA/PIA-023(a)

December 11, 2020

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Infrastructure Security Division (ISD) maintains the CISA Gateway, a system formerly known as Infrastructure Protection (IP) Gateway, a web-based portal that supports the collection, analysis, and dissemination of critical infrastructure information. CISA published the original IP Gateway Privacy Impact Assessment (PIA) in 2015 and provided a subsequent update in 2018. CISA is updating and reissuing DHS/CISA/PIA-023 to document a new sign-on mechanism, an interface with a two-factor authentication system, migration to a cloud environment, a system name change from IP Gateway to CISA Gateway, and to reflect the agency name change from the National Protection and Programs Directorate (NPPD) to CISA. This PIA reflects these updates and fully re-assesses privacy risks and mitigations for the system.

Overview

CISA ISD leads the coordinated national effort to protect critical infrastructure[1] from all hazards by managing risk and enhancing resilience through collaboration with federal, state, local, tribal, territorial, and private sector partners in the critical infrastructure community. In support of this mission, ISD developed the CISA Gateway to encompass numerous applications[2] and tools maintained by ISD and other components within CISA to reflect the reorganized nature of CISA as a new operational component of DHS. The primary purpose of the CISA Gateway is to provide a framework for enhanced sharing of infrastructure information. The CISA Gateway is a web-based portal that supports the collection, analysis, and dissemination of infrastructure information.

Applications on the CISA Gateway will be accessed by logging in to the main CISA Gateway user interface using two-factor authentication (2FA). Access to the CISA Gateway is restricted to only federal, state, local, tribal, and territorial critical infrastructure mission partners that possess homeland security responsibilities, have a valid "need to know,"[3] and have completed Protected Critical Infrastructure Information (PCII)[4] authorized user training.

---

[1] Section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. § 5195c(e)) defines critical infrastructure as namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

[2] "Application" refers to a single capability under the three capability groups (i.e., Data Collection and Web-Based Dashboards, Information Sharing and Training Tools, and Administrative, Management, and Reporting Capabilities) described in the Overview section. The term "application" does not refer to a separate system or sub-system.

[3] A federal government user's "need to know" is determined by whether or not access to the information is necessary in order to perform his or her official duties. For state and local government users, their particular states define what is considered to be a valid "need to know" for access to the CISA Gateway.

[4] PCII is a program that protects infrastructure information voluntarily shared with DHS to be used for homeland security purposes. As authorized by the Critical Infrastructure Information Act of 2002, PCII in the Government's hands is protected from disclosure. *See* Critical Infrastructure Information Act of 2002, *available at*: http://www.dhs.gov/sites/default/files/publications/CII-Act_508.pdf. Also *see* U.S. DEPARTMENT OF

Individuals may request access to the CISA Gateway by completing the CISA Gateway Account Request form via the CISA Gateway registration website at https://gateway.cisa.gov. The CISA Gateway Account Request Form requests various data elements, which differ based on the type of applicant (i.e., federal employee, federal contractor, state government employee, state government contractor, local government employee, or local government contractor) that is requesting access to the CISA Gateway.

CISA Gateway Capability Groups

The CISA Gateway provides users with access to a number of applications supporting activities such as data collection and management, operational scheduling, report management, and analysis for comprehensive risk assessment, management/mitigation, and contingency planning. For the sake of clarity, the applications that reside on the CISA Gateway can be grouped into three main capabilities:

- Data Collection and Web-Based Dashboards;
- Information Sharing and Training Tools; and
- Administrative, Management, and Reporting Capabilities.

Capability Group 1: Data Collection and Web-Based Dashboards

- The purpose of the data collection and web-based dashboards is to collect and display data for the Protective Security Advisors (PSA),[5] Sector Specific Agencies (SSA),[6] and the State, Local, Tribal, and Territorial (SLTT) communities. These capabilities allow for analysis of performance and review of vulnerabilities of Critical Infrastructure (CI). The focus is on physical security, cybersecurity, security force, security management, information sharing, protective measures, and internal and external dependencies. The web-based dashboards are used to convey, track, manage, and graphically display information collected by the PSAs or through incident reporting. Geospatial information is collected through data

HOMELAND SECURITY, CYBERSECUIRTY AND INFRASTRUCTURE SECUIRTY AGENCY, PRIVACY IMPACT ASSESMENT FOR THE PROTECTED CRITICAL INFRASTRUCTURE INFORMATION PROGRAM, DHS/NPPD/PIA-034 (2019), *available at*: https://www.dhs.gov/privacy-documents-cisa.

[5] PSAs facilitate field activities in coordination with other DHS offices. The PSA Program maintains a robust operational field capability by conducting assessments of nationally significant critical infrastructure through Enhanced Critical Infrastructure Protection (ECIP) security surveys; site assistance visits and incident response; and providing access to infrastructure security and resilience resources, training, and information.

[6] SSAs are federal departments or agencies designated under Presidential Policy Directive-21 (PPD-21) to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. *See* PPD-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013) *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

collection functions and updated to DHS geospatially-enabled data. This data is then used to display the reports and maps of CI facilities in a query.

Capability Group 2: Information Sharing and Training Tools

- The information sharing and training functionality includes dynamic sharing of data and information sources across the critical infrastructure community, including facility owners and operators, and SLTT community partners. The information sharing tools enable stakeholders to easily access, search, retrieve, visualize, analyze, and export infrastructure data and protective measures. Data purview restrictions and access controls are managed within the individual applications based on a user's need to know. The movement of information and data through the communication channels across the organization (from field personnel to Headquarters), along with the short and long-term storage capabilities, allows the archival, retrieval, and handling of data at will. The ability to provide simple knowledge management provides relevant material for designing training content for both employees as well as stakeholders.

Capability Group 3: Administrative, Management, and Reporting Capabilities

- The administrative, management, and reporting functionality is used to schedule, track, coordinate, and maintain activities in the field. This set of capabilities allows both field personnel and CISA leadership at Headquarters to provide performance management metrics and quickly assess impacts of missions in the field. In addition, the CISA Gateway provides the ability to connect personnel at Headquarters with personnel in the field who are performing the critical functions to protect our Critical Infrastructure.

CISA Gateway applications[7] may collect business contact information from users and other Points of Contact (POC). POCs may include, but are not limited to, private sector partners or stakeholders associated with specific infrastructure assets. CISA may use this information to communicate with facilities in support of its infrastructure protection mission. For example, during an event or incident, such as an attack or natural disaster, CISA may need to contact facility owners or operators to convey information to help protect their infrastructure. The information collected from POCs is limited to business contact information, such as full name, email address, office phone number, cell phone number, and business address.

This PIA serves as an update and a replacement for DHS/NPPD/PIA-023 PIA "Infrastructure Protection (IP) Gateway," dated September 11, 2018. Since the 2018 PIA, the

[7] See Appendix A for the current list of all CISA Gateway applications divided into separate CISA Gateway Capability Groups.

renamed CISA Gateway has been updated to incorporate a new sign-on mechanism, to interface with a two-factor authentication system, and has been migrated to a cloud environment.

Initially, CISA Gateway will continue to use Homeland Security Information Network (HSIN)[8] for system access during its implementation phase as described in the 2018 update of DHS/NPPD/PIA-023 for IP Gateway. Once CISA Gateway receives its Authority to Operate (ATO), it will migrate to DHS' implementation of Application Authentication (AppAuth) for Single Sign On services for authentication, enabling DHS users across the Department to log on to enterprise applications using their normal component login credentials. The system will abide by and inherit the privacy controls that are currently in place for the AppAuth system as documented in its respective PIA.[9]

Users outside of DHS will no longer use HSIN for access. Non-DHS users will log on using 2FA with a username and password which is authenticated via a five (5) or six (6) digit verification number sent via text or email to the contact point that was placed on file when the user originally registered his or her account.

The system is also adding an application programming interface (API) Connection[10] out to the CISA Cybersecurity Division's Tardis application. Tardis is an Event and Incident ticketing platform which is currently a part of the Incident Management System (IMS) of the National Cybersecurity Protection System,[11] which, like CISA Gateway, also requires PCII training for access. The sharing of PCII training records will take place through a Memorandum of Understanding (MOU) between the CISA Gateway System Owner and the Tardis System Owner in order to allow Tardis users to pull their PCII Training statistics from the CISA Gateway to ensure that the Tardis users have the requisite up-to-date PCII training record to access the Tardis application.

---

[8] See U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR HSIN RELEASE 3 USER ACCOUNTS, DHS/ALL/PIA-061-1 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR APPLICATION AUTHENTICATION SYSTEM, DHS/ALL/PIA-060 (2018), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[10] An API is a computing interface which defines interactions between multiple software intermediaries. CISA Gateway will be an API connection to send an encrypted PCII training status in a "yes/no" type response over to the Tardis application.

[11] See U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, PRIVACY IMPACT ASSESSMENT FOR THE NATIONAL CYBERSECURITY PROTECTION SYSTEM (NCPS), DHS/CISA/PIA-026 (2012), *available at* https://www.dhs.gov/privacy-documents-cisa.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

CISA Gateway is primarily used to collect non-privacy sensitive infrastructure information as authorized by Section 2202 of the Cybersecurity and Infrastructure Security Agency Act of 2018.[12] Furthermore, CISA's PCII program, authorized by the Critical Infrastructure Information Act of 2002,[13] controls the protection of the majority of the critical infrastructure information collected and maintained within the CISA Gateway.

Presidential Policy Directive-21 (PPD-21) Critical Infrastructure Security and Resilience, issued in 2013, specifically directs DHS to:

1) In coordination with SSAs and other federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure; and

2) Conduct comprehensive assessments of the vulnerabilities of the nation's critical infrastructure in coordination with SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators.

In support of PPD-21 and the CISA Act of 2018, CISA/ISD employs the CISA Gateway, which provides federal, state, and local government critical infrastructure mission partners with various data collection, analysis, and response tools in order to enhance critical infrastructure protection.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

CISA collects PII from individuals for the purpose of granting access to the IP Gateway. This collection is covered by the DHS system of records notice titled, DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[14] CISA also collects PII to provide customer support to users through the CISA Gateway Help Desk. This collection is covered under DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System.[15]

---

[12] Pub. L. No. 115-278, 132 Stat. 4168 (2018) (codified at 6 U.S.C. § 652).
[13] Pub. L. No. 107-296, 116 Stat. 2150 (Nov. 25, 2002) (codified as amended at 6 U.S.C. § 671 et seq.).
[14] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792, (Nov. 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.
[15] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (Nov. 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm.

In addition to the collections described above, the CISA Gateway may also maintain limited business contact information on critical infrastructure POCs. This information, however, is not filed or retrieved by the individual's PII and therefore is not covered by the Privacy Act. POC information is generally filed and retrieved by the name of a facility or other asset with which the individual is associated.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A system security plan is currently being drafted for the CISA Gateway and as of November 2020, the date as to when an Authority to Operate (ATO) will be issued is still undetermined as security controls brought up during system assessment are being remediated prior to implementation.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

User registration records are maintained in accordance with NARA's General Retention Schedule 3.2 – Information Systems Security Records, and records created through the CISA Gateway Help Desk (IT Customer Service Files) are maintained in accordance with NARA's General Retention Schedule 24 – Information Technology Operations and Management Records.

Additionally, NARA Job No. N1-563-08-36 covers the PCII submitted and maintained through the CISA Gateway, and NARA Job No. N1-563-04-09 covers the critical infrastructure submissions that do not meet the requirements for PCII.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

In its previous iteration as IP Gateway, the system went through the PRA approval process. The CISA Gateway's PRA package includes both the CISA Gateway Account Request Form (used for CISA Gateway user registration) and the voluntary CISA Gateway Customer Satisfaction Survey. The PRA package received an OMB Control number of 1670-0009. This package was approved to include the necessary changes to the system which would evolve to be CISA Gateway, and the form used for user registration continues to be valid for CISA Gateway moving forward.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

In order to register for access to the CISA Gateway, individuals are required to provide certain information via the online CISA Gateway Account Request Form. This form requests various data elements, which differ based on the type of applicant (i.e., federal employee, federal contractor, state government employee, state government contractor, local government employee, or local government contractor) requesting access to the CISA Gateway. The information collected by the CISA Gateway Account Request Form is outlined below.

All applicants must provide the following information:

- Name;
- U.S. citizen (yes/no);
- Employee type (federal employee, federal contractor, state government employee, state government contractor, local government employee, or local government contractor);
- Role requested (e.g., Assessor/Analyst);
- Role in organization;
- Do they hold any regulatory or rulemaking responsibilities (yes/no);
- Work address;
- Work email;
- Work phone number;
- Mobile phone number (optional);
- Does their organization provide annual Cyber Security and Awareness Training (yes/no);
- Organization's Cyber Security Training Date;
- Their need to know (as verified by CISA Gateway Administrators described below);
- For which state they are requesting CISA Gateway access (applicant may also request to restrict their access to a particular county, city, or zip code within that particular state);

- PCII trained (yes/no);
- PCII certification number; and
- How they plan to use this information (Analysis or PCII Program coordination; incident planning; emergency response; performing assessments; other).

All additional information requested through the CISA Gateway Account Request Form is dependent upon the type of employee requesting access:

- *Federal employees*: Must provide their department or agency; component; work supervisor's first and last name, email address and phone number; and their ISD Sponsor's[16] first and last name, email address, and phone number.
- *Federal contractors*: Must provide the department or agency they support; component; contractor representative's first and last name, email address and phone number; contracting company's name and address; and their ISD Sponsor's first and last name, email address, and phone number.
- *State and local government employees*: Must provide their state government name and agency.
- *State and local government contractors*: Must provide their state government name; the government agency they support; contractor representatives' first and last name, email address, and phone number; and their contracting company's name and address.

Once a federal, state, or local government critical infrastructure mission partner submits his or her CISA Gateway Account Request Form, it is electronically sent to a CISA Gateway Administrator. CISA Gateway Administrators are responsible for vetting potential CISA Gateway users' need to know and for managing their level of access to CISA Gateway data. These CISA Gateway Administrators are located at both the federal and state levels and are responsible for managing the accounts of CISA Gateway users who work in their community (i.e., federal, state, or local government users). For example, if a CISA Gateway applicant is a Department of Defense (DOD) employee, then a CISA Gateway Administrator working within DOD will be assigned to review/vet the applicant's CISA Gateway Account Request Form and determine what level of access (e.g., state, county, city, or zip code-wide), if any, the applicant should receive. There is no difference in CISA Gateway user roles or access rights between CISA Gateway Administrators at the federal-level versus those working at the state-level. For more information regarding the

[16] Federal government employees and contractors must provide an ISD Sponsor's name and contact information in order to register for access to the CISA Gateway. This information is collected so that CISA Gateway Administrators may contact ISD Sponsors to ensure that the requesting federal government employee or contractor has a valid need to know for access to the CISA Gateway.

different levels of CISA Gateway access and data partitioning, please see Section 8.3 of this PIA. CISA Gateway Administrators at the state-level are appointed by state HSAs and are required, as are all CISA Gateway Administrators, to take the DHS-provided CISA Gateway module training to ensure they understand the requirements to establish a valid need to know for state and local government critical infrastructure mission partners.

When a federal, state, or local government critical infrastructure mission partner initially submits his or her CISA Gateway Account Request Form, it is automatically sent to a CISA Gateway Administrator, working within CISA/ISD, to review whether or not the applicant has completed PCII Authorized User Training. The review of an applicant's PCII Authorized User Training must be performed by CISA Gateway Administrators working within CISA/ISD because Administrators are provided with access to the list of PCII Authorized Users maintained through the Protected Critical Infrastructure Information Program (PCII).[17] In order to receive access to the CISA Gateway, all applicants must be PCII Authorized Users because certain surveys and assessments that are conducted using CISA Gateway are secured as PCII. If applicants are not PCII Authorized Users, then they will be redirected to PCIIMS in order to take the training before being granted an CISA Gateway account. This PCII Authorized User Training covers the consequences of loss or misuse of PCII data, including criminal and administrative penalties.

Upon review of the CISA Gateway applicant's PCII training status, the applicant's CISA Gateway Account Request Form is automatically submitted to their assigned CISA Gateway Administrator for review based on their community (i.e., federal, state, or local government). Currently, only approved DHS/CISA employees that meet the CISA Gateway's access requirements are provided with access to the national view, since DHS/CISA leads the national effort to protect and enhance the resilience of the nation's critical infrastructure.

If the assigned CISA Gateway Administrator determines that the federal, state, or local government critical infrastructure mission partner meets the necessary requirements for access to CISA Gateway, then the applicant is approved for a CISA Gateway user account. During its initial implementation phase, individuals with approved CISA Gateway user accounts will continue to use HSIN as the method for identity authentication. As described in the 2018 update of this PIA, once the applicant is approved, he or she will be prompted to complete the HSIN Registration Process if he or she does not currently have an account. Once a CISA Gateway account is created, when a user attempts to log into his or her CISA Gateway account, it will go through the HSIN portal for identity proofing and then log the user directly in to the CISA Gateway.

Once fully implemented and the system is granted its ATO, CISA Gateway will migrate to

[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECUIRTY AND INFRASTRUCTURE SECUIRTY AGENCY, PRIVACY IMPACT ASSESSMENT FOR PROTECTED CRITICAL INFRASTRUCTURE INFORMATION Program, DHS/CISA/PIA-034 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-cisa.

AppAuth to provide identity verification for only internal DHS users accessing the CISA Gateway. Once the applicant is approved, the DHS user will be able to access the system via Personal Identity Verification (PIV) card authentication and authorization. Once a CISA Gateway account is created, when a DHS user attempts to log into his or her CISA Gateway account, AppAuth will seamlessly allow for identity proofing and then log the user directly into the CISA Gateway.

External to DHS users will not be able to utilize AppAuth. Once the use of HSIN for identity authentication is discontinued, a 2FA method will be established to facilitate non-DHS users' access. The non-DHS user will go through a PCII approval process and will register to the CISA Gateway using the registration website. Once non-DHS users are registered, the CISA Gateway Help Desk is alerted and the non-DHS users' information is stored in the CISA Gateway along with Active Directory. Help Desk personnel will check the requested non-DHS users incoming attributes that were entered during registration and then change their status to "email verification" manually. Once the non-DHS user receives the email verification step, he or she completes the registration by establishing password and security questions. At this point, the individual's status will be active and he or she can access the application(s) assigned via the authentication method he or she has just established. Upon logging into the CISA Gateway for the first time, users will be prompted to complete the CISA Gateway user training. Training must be completed before full access to the CISA Gateway is permitted because it provides users with a general overview of the system and its various tools and applications.

CISA may also collect business contact information from critical infrastructure POCs, which is accessible through the CISA Gateway. This business contact information includes full name, email address, office phone number, cell phone number, and business address.

Lastly, along with its responsibilities with registration, the CISA Gateway provides a Help Desk as an information and assistance resource for troubleshooting problems with the CISA Gateway. The CISA Gateway Help Desk provides a single point of contact for both internal and external stakeholders and partners for technical questions and assistance on current tools and applications within the CISA Gateway. The CISA Gateway Help Desk may collect basic contact information from individuals in order to provide customer support via phone or email. This contact information includes the individual's name, work email, and work phone number.

2.2 What are the sources of the information and how is the information collected for the project?

The information maintained in the CISA Gateway is received directly from the individual to whom it pertains. Sources primarily include federal employees, federal contractors, state government employees, state government contractors, local government employees, and local government contractors. Critical Infrastructure POC information may be collected directly from the individual or may be provided by individuals designated to act on behalf of the critical

infrastructure facility or private sector entity via other CISA programs and uploaded to the CISA Gateway. Critical infrastructure information maintained on the CISA Gateway may come from a variety of different sources but does not include PII.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The CISA Gateway may include information collected from publicly available sources for the purpose of completing and verifying basic identifying infrastructure information in submitted site records and for developing background reports on infrastructure that will be later visited by CISA personnel. This collection, however, does not include any PII.

2.4 Discuss how accuracy of the data is ensured.

To ensure accuracy, CISA/ISD collects registration information directly from individuals that have or are seeking access to the CISA Gateway. Contact information is collected directly from critical infrastructure POCs or individuals designated to act on behalf of the critical infrastructure facility or private sector entity.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of the CISA Gateway collecting inaccurate PII or over collecting PII during its registration process.

Mitigation: This risk is mitigated. The CISA Gateway only collects business contact information directly from individuals for the limited purposes of registering users for the CISA Gateway, providing quality support via the CISA Gateway Help Desk, and gathering critical infrastructure POC information.

Registration for users via AppAuth is subject to information derived from DHS employees/contractors. When an individual is onboarded, his or her human resource information is solicited by personnel security and provided to be passed on for insertion into the DHS Active Directory. AppAuth pulls the information from those active directories. All changes made in those active directories are synced automatically in AppAuth when they are made in the active directories.

After the PCII approval process, the non-DHS User will register with the CISA Gateway using the registration website. Once registered, the CISA Gateway Help Desk is alerted and the non-DHS information is stored in the CISA Gateway along with Active Directory. Help Desk personnel will check the requested non-DHS users incoming attributes that were entered during registration and then change their status to “email verification” manually. Once the user receives

the email verification step, he or she completes the registration by verifying his or her information and establishing password and security questions prior to accessing the application(s) in the CISA Gateway.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CISA collects PII from federal, state, and local government critical infrastructure mission partners during the CISA Gateway registration process so that CISA can create and manage CISA Gateway user roles and accounts. Once users are provided with an account, these individuals may access a variety of applications to conduct comprehensive data collection and analysis consistent with their need to know. Specifically, CISA Gateway enables federal, state, and local government critical infrastructure mission partners to manage information about the infrastructure in their communities for risk management, infrastructure protection, event planning, and incident response activities.

The following user roles determine what data users may access within the CISA Gateway.

- *Administrator*: Administrators may view the CISA Gateway's entire suite of capabilities, in addition to having the responsibility for managing the accounts of the CISA Gateway users who work in their community of practice. Administrators have read and write access to the User Management capability, which allows them to determine a user's level of access and privileges within the CISA Gateway. They also have read and write access to the surveys and assessments they have conducted, as well as read-only access to completed visits within their community. They have read-only access to critical infrastructure data for their community throughout a series of other CISA Gateway tools, as well as read and write access to planning capabilities.
- *Assessor*: Assessors conduct critical infrastructure site surveys and assessments. Assessors have read and write access to the surveys and assessments they have conducted, as well as read-only access to completed visits within their community. They also have read-only access to critical infrastructure data related to their community through a variety of CISA Gateway tools.
- *Analyst*: Analysts are responsible for accessing and analyzing CISA Gateway data. Analysts have read-only access to completed surveys and assessments within their community. They also have read-only access to critical infrastructure data related to their community through a variety of CISA Gateway tools.

The CISA Gateway Help Desk also collects PII from current and potential users in order to manage CISA Gateway user accounts and to provide technical support.

Lastly, CISA uses critical infrastructure POC information in order to facilitate communications with stakeholders related to critical infrastructure security and resilience.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, the CISA Gateway does not use any technology to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, there are no other DHS components with assigned roles and responsibilities within the CISA Gateway.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that users may access and use information in CISA Gateway applications beyond the scope of their mission.

Mitigation: This privacy risk is mitigated. CISA Gateway Administrators assess all potential users to ensure they possess a valid need to know for access as well as limit their access to only the applications necessary for them to perform their homeland security responsibilities. CISA further mitigates this risk by ensuring that user PII is only accessible to the CISA Gateway Administrators who require access to manage system users. Through this role-based access process, CISA minimizes the risk of unauthorized access to CISA applications or misuse of PII. The *CISA Gateway System-Use Disclaimer*[18] also appears prior to logging into the system and requires all users to acknowledge certain conditions before gaining access to the CISA Gateway. This disclaimer dictates how data may be used and warns users that misuse may be punishable by civil or criminal penalties.

The CISA Gateway further grants access to federal, state, and local government critical infrastructure mission partners based on location, including state, county, city, and zip code partitioning options. This ensures that each user has access to only the data for which he or she has a need to know in order to perform his/her homeland security responsibilities. For example, a Virginia state user only has access to CISA Gateway data for Virginia and will not be able to access any other state's data. This partitioning extends to the entire suite of applications. Currently, only approved CISA employees that meet the system access requirements are provided with access

[18] See Attachment 3.

to the national view as DHS/CISA leads the national effort to protect and enhance the resilience of the nation's critical infrastructure.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The CISA Gateway Account Request Form includes a Privacy Act Statement[19] for individuals requesting access to the CISA Gateway and to individuals contacting the CISA Gateway Help Desk before submitting any personal identifiable information to CISA. For individuals who proactively contact or contact CISA via phone, notice is provided at https://www.cisa.gov/cisa-gateway and the Privacy Policy page.

Additionally, CISA provides notice through the re-issuing of this PIA and through the publication of the DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORNs.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All PII is submitted on a voluntary basis and, as such, individuals may elect not to participate. An individual's PII is only used for the purposes of registration, CISA Gateway Help Desk support, or contacting POCs as necessary. Users of the CISA Gateway may request to update or remove their information by contacting the CISA Gateway Help Desk. Help Desk staff will coordinate the request with the CISA Gateway Program Manager. The Program Manager will work in coordination with the CISA Office of the Chief Privacy Officer to ensure the updates or removal of the requested information is in accordance with DHS policy.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk CISA Gateway Users will not be provided with adequate notice as to how their PII will be used.

Mitigation: This privacy risk is mitigated. CISA provides Privacy Act Statements to individuals requesting access to the CISA Gateway via the CISA Gateway Account Request Form and to individuals contacting the CISA Gateway Help Desk before they submit any personal information to CISA. Notice is also provided via this PIA update and the applicable SORNs: DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System and

[19] See Attachment 1.

DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

User registration records are maintained until the business use ceases, in accordance with NARA's General Retention Schedule 3.2 – Information Systems Security Records.[20]

Records created through the CISA Gateway Help Desk (IT Customer Service Files) are maintained for one year after they are superseded or obsolete, in accordance with NARA's General Retention Schedule 3.1 – General Technology Management Records, Item 040 - Information technology oversight and compliance records.[21]

Additionally, CISA has a retention schedule approved by NARA for PCII submitted and maintained through the CISA Gateway under NARA Job No. N1-563-08-36.[22] In addition, the NARA approved retention schedule, NARA Job No. N1-563-04-09,[23] covers the critical infrastructure submissions that do not meet the requirements for PCII.

CISA is currently working on a comprehensive records schedule for all other records generated and maintained by the CISA Gateway system.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that PII may be retained by CISA Gateway longer than necessary.

Mitigation: The privacy risk is partially mitigated. CISA only retains information for as long as necessary and relevant to the purposes of CISA Gateway. There are minimal risks that CISA Gateway will retain PII for a longer time period than is relevant and necessary under its

[20] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, GENERAL RECORDS SCHEDULE NUMBER 3.2, INFORMATION SYSTEMS SECURITY RECORDS (2016), *available at* https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf.
[21] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, GENERAL RECORDS SCHEDULE NUMBER 3.1, GENERAL TECHNOLOGY MANAGEMENT RECORDS (2017), *available at* https://www.archives.gov/files/records-mgmt/grs/grs03-1.pdf.
[22] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST RRECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-563-08-36, U.S. DEPARTMENT OF HOMELAND SECURITY, PROTECTED CRITICAL INFRASTRUCTURE INFOMRATION MANAGEMENT SYSTEM (PCIIMS) RECORDS (2008), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0602/n1-563-08-036_sf115.pdf.
[23] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST RRECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-563-04-09, U.S. DEPARTMENT OF HOMELAND SECURITY, PROTECTED CRITICAL INFRASTRUCTURE INFOMRATION MANAGEMENT SYSTEM (PCIIMS) RECORDS (2004), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-04-009_sf115.pdf.

approved records retention schedules. Audits and ongoing vigilance are applied to verify adherence to applicable records retention schedules. In addition, Section 8.0 of this PIA update details the security measures used to safeguard CISA Gateway information throughout its lifecycle.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CISA critical infrastructure POC information and infrastructure-related data is shared through the CISA Gateway with DHS employees as well as state and local government critical infrastructure mission partners who possess homeland security responsibilities, have a valid need to know, and have completed PCII Authorized User Training.

The CISA Gateway will also establish an API Connection to share information with the CISA Cybersecurity Division's Tardis application. Tardis is an Event and Incident ticketing platform which is currently a part of the Incident Management System (IMS) of the National Cybersecurity Protection System which, like the CISA Gateway, also requires PCII training for access. The sharing of PCII Training records will take place through a Memorandum of Understanding (MOU) between the CISA Gateway System Owner and the Tardis System Owner in order to facilitate and automate the verification of PCII training status for the Tardis system users. No PII will be shared between the systems. Only a "Yes/No" response as to whether the individuals have completed PCII training and the expirations date for training validity.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

CISA does not share any Privacy Act-covered information outside of DHS from the CISA Gateway. CISA collects PII from individuals for the purpose of granting access to the CISA Gateway and to provide customer support to users through the CISA Gateway Help Desk. These information collections are covered by the DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORNs and are not shared outside of DHS.

However, the CISA Gateway also maintains limited business contact information on critical infrastructure POCs. As noted in Section 1.2, this information is not filed or retrieved by the individual's PII and therefore is not covered by the Privacy Act. POC information is generally filed and retrieved by the name of a facility or other asset with which the individual is associated. This critical infrastructure POC information is the only PII shared outside of CISA via CISA

Gateway with DHS employees as well as federal, state, and local government critical infrastructure mission partners who possess homeland security responsibilities, have a valid need to know, and have completed PCII Authorized User Training.

6.3 Does the project place limitations on re-dissemination?

User PII collected for CISA Gateway registration purposes cannot be re-disseminated outside of CISA because the information is collected for the sole purpose of granting access to the CISA Gateway.

Some PII associated with CISA critical infrastructure POCs is intertwined with PCII contained within the CISA Gateway. Re-dissemination limitations are consistent with the safeguarding and handling requirements of PCII, which is only shared with PCII Authorized Users that possess a need to know. All other data within the CISA Gateway is, at most, Sensitive but Unclassified (SBU) and, as such, is only to be shared with other federal, state, or local entities that possess a need to know.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The CISA Gateway audits all user access to its data. As such, a record is maintained, within the CISA Gateway system itself, and stored in an encrypted database which includes the name of the user, the date of access, and the data accessed. No one person or entity stores such records on personal drives or other locations; these records reside within the system itself.

CISA does not share any Privacy Act-covered information outside of DHS from the CISA Gateway.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that POC information maintained on the CISA Gateway will be shared with individuals that do not possess a need to know.

Mitigation: This privacy risk is mitigated. CISA mitigates this risk by having CISA Gateway Administrators assess potential CISA Gateway users prior to access being granted to ensure that all CISA Gateway users possess a valid need to know for access to the POC information maintained on the CISA Gateway.

This risk is further mitigated by CISA Gateway Administrators limiting users' system access to only the data for which the users have a need to know in order to perform their homeland security responsibilities, per PCII data protection requirements. To do this, CISA Gateway Administrators assign user roles and partition data based on location and user need to know. The CISA Gateway system user roles (e.g., Administrator, Assessor, or Analyst) determine which applications a user may view within the CISA Gateway. Meanwhile, by partitioning data, CISA

Gateway Administrators can limit federal, state, and local government users' access based on their location, to include state, county, city, and zip code partitioning options. As a result, CISA Gateway users do not have access to any PII for which they do not possess a need to know. This risk is also mitigated by the CISA Gateway Disclaimer to which all users of the system are required consent to before logging in. This disclaimer dictates how data from the system may be used and warns users that misuse may be punishable by civil or criminal penalties.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

CISA Gateway users are able to access their PII via the account management tool or by contacting the CISA Gateway Help Desk via email at CISA-gatewayhelpdesk@cisa.dhs.gov or by telephone at (866) 844-8163. Critical infrastructure POCs do not have direct access to their information through the CISA Gateway. However, POCs have an ongoing relationship with CISA and can access and correct information that was voluntarily provided to the agency. For example, a POC may choose to contact CISA to ensure that information on his/her facility, including his/her contact information, is accurate.

Individuals may also request access to information about themselves by submitting a Freedom of Information Act (FOIA) or Privacy Act request to the following address:

DHS Privacy Office
Privacy Office, Mail Stop 0655
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Ave SE
Washington, DC 20528-065

These requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Directions on how to submit a FOIA or Privacy Act request can be found at https://www.dhs.gov/dhs-foia-handbook.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

CISA Gateway users may update their contact information via the account management tool or by contacting the CISA Gateway Help Desk. POCs may update erroneous information by making a request to the CISA division that collected the information from them. Instructions on how to correct inaccurate or erroneous information are provided in this PIA and through guidance issued by the CISA Gateway program office.

Users may also write to the Privacy Office at the address listed in Section 7.1 above to have inaccurate or erroneous PII corrected.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of the procedures to correct information through this PIA and the DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORNs. Users may also contact the CISA Gateway Help Desk during business hours. Help Desk contact information is readily available on the CISA Gateway log-in screen.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Individuals may be unaware of or not understand their redress options.

Mitigation: This is privacy risk is mitigated. Most PII maintained within CISA Gateway pertains to CISA Gateway users, in which case, those users have the ability to access and correct their data via the account management tool or by contacting the CISA Gateway Help Desk. Although POCs do not have direct access to information, most POCs can update or correct their data through ongoing working relationships with CISA and its respective divisions. Redress will be provided as described above in Sections 7.1 and 7.2. Notice of redress procedures are also provided in the DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORNs. Contact information for the CISA Gateway Help Desk is readily available on the CISA Gateway log-in screen.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The CISA Gateway uses a number of continuous monitoring tools to maintain a secure baseline and to prevent unauthorized access, including centralized logging and vulnerability scanning tools. The system has also been subject to multiple audits by the Government Accountability Office (GAO) and the DHS Office of Inspector General (OIG) regarding the collection, security, and use of data gathered from across all 16 critical infrastructure sectors. In addition, DHS policy requires that systems implement auditing at the user level and regularly analyze audit logs to determine misuse or abuse. The likelihood of unauthorized access is mitigated through technical controls including firewalls, intrusion detection, encryption, access control lists, system hardening techniques, and other security measures. All implemented controls meet federal and DHS requirements governing information assurance.

The CISA Office of Privacy maintains an internal inventory of all CISA Gateway applications and works with the CISA Gateway Program on a continual basis to review and assess new applications, as well as changes to existing applications, to ensure that proper privacy compliance documentation is in place and that all privacy risks are being managed appropriately.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Users outside of DHS with access to the CISA Gateway will not receive privacy training from DHS. However, all DHS users (employees and contractors) undergo DHS privacy training, which includes a discussion of the DHS Fair Information Practice Principles (FIPPs) and instructions on handling PII in accordance with the FIPPs and DHS privacy policy. Additionally, all DHS and contractor personnel must complete annual privacy refresher training to retain system access. Security training is also provided to DHS personnel on an annual basis, which helps to maintain awareness for safeguarding PII. DHS reports on employees and contractors who receive IT security and privacy training as required by the Federal Information Security Management Act (FISMA) of 2002.

In addition, certain information maintained in the CISA Gateway is considered PCII. As a result, all CISA Gateway users are required to take PCII Authorized User Training before they are granted access. This training provides CISA Gateway users with an understanding of proper handling and safeguarding techniques for PCII.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The CISA Gateway Administrator assigned to review the applicant's CISA Gateway Account Request Form is responsible for ensuring that the user's access is limited to only the data for which the user has a need to know, per PCII data protection requirements, before the applicant is granted access to the CISA Gateway. CISA Gateway Administrators are responsible for vetting and granting access for requesting homeland security professionals to one of three user roles (Administrator, Assessor, or Analyst as described in Section 3.1).

Additionally, DHS has well-established and comprehensive processes to enhance information security and minimize possibilities for unauthorized access. DHS personnel adhere to internal information security policies. Furthermore, robust auditing measures and technical safeguards will help monitor unauthorized access and attempted access. To reduce the risk of a data breach, proactive monitoring of logs will identify potential incidents as early as possible, and audit trails will be maintained to facilitate investigation of incidents in accordance with DHS Privacy Incident Handling Guidance. Regularly scheduled risk assessments will be performed on

the security controls to identify potential vulnerabilities, including technical, managerial, and physical security access.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All information sharing agreements are developed by the program manager and the system owner in coordination with the CISA Data Governance Board and the CISA Office of Privacy. In addition, the CISA Office of Chief Counsel reviews agreements, access, MOUs, and uses of information, as appropriate.

Contact Official

Iesha Alexander
CISA Gateway Program Manager, Office of Infrastructure Assessments and Analysis
Infrastructure Security Division/ Cybersecurity and Infrastructure Security Agency
(703) 235-9305
Iesha.Alexander@cisa.dhs.gov

Responsible Official

Gregory Bird
Mission Systems Branch Chief, Office of Infrastructure Assessments and Analysis
Infrastructure Security Division/ Cybersecurity and Infrastructure Security Agency

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

ATTACHMENT 1

CISA Gateway Privacy Act Statement

Authority: 44 U.S.C. § 3101 and 44 U.S.C. § 3534 authorize the collection of this information.

Purpose: DHS will use this information to create and manage your user account and grant access to the CISA Gateway.

Routine Use: This information may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974. This includes using the information, as necessary and authorized by the routine uses published in DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 Fed. Reg. 70792.

Disclosure: Furnishing this information is voluntary; however, failure to provide the information requested may delay or prevent DHS from processing your access request.

ATTACHMENT 2

CISA Gateway Help Desk Privacy Act Statement

Authority: 5 U.S. C. § 301 and 44 U.S.C. § 3101 authorize the collection of this information.

Purpose: DHS will use this information to confirm your CISA Gateway user role and respond to your questions.

Routine Use: This information may be disclosed as generally permitted under 5 U.S.C. §552a(b) of the Privacy Act of 1974, as amended. This includes using the information, as necessary and authorized by the routine uses published in DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System of Records November 25, 2008, 73 Fed. Reg. 71659.

Disclosure Furnishing this information is voluntary; however, failure to provide any of the information requested may prevent the CISA Gateway Help Desk from providing assistance or answering your questions.

ATTACHMENT 3

CISA Gateway System-Use Disclaimer

The following disclaimer is displayed for and must be accepted by all users prior to accessing the CISA Gateway:

You are about to access a U.S. Department of Homeland Security computer system. This computer system and data therein are property of the U.S. Government and provided for official U.S. Government information and use. There is no expectation of privacy when you use this computer system. The use of a password or any other security measure does not establish an expectation of privacy. By using this system, you consent to the terms set forth in this notice. You may not process classified national security information on this computer system. Access to this system is restricted to authorized users only. Unauthorized access, use, or modification of this system or of data contained herein, or in transit to/from this system, may constitute a violation of section 1030 of title 18 of the U.S. Code and other criminal laws. Anyone who accesses a federal computer system without authorization or exceeds access authority, or obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on the computer system, may be subject to penalties, fines, or imprisonment. This computer system and any related equipment is subject to monitoring for administrative oversight, law enforcement, criminal investigative purposes, inquiries into alleged wrongdoing or misuse, and to ensure proper performance of applicable security features and procedures. DHS may conduct monitoring activities without further notice.

APPENDIX A – CISA Gateway Applications (*last updated December XX, 2020*)

Data Collection and Web-Based Dashboards

Data Viewer - The Data Viewer allows users to view data collected through the Automated Critical Asset Management System (ACAMS), a decommissioned program. The ACAMS system was used by state and local government agencies to collect critical infrastructure information to support state and local homeland security duties.

Dependency/Dependency Profile Editor – The Dependency tools provide a rapid visual representation of the relationships and dependencies between critical infrastructures. The dependency profile editor stores general definitions about the inputs and outputs of a critical infrastructure facility, system, or area.

Events and Incidents - Events and Incidents is a reference capability designed to dynamically contain important information such as contacts, documents, resources, and links for Steady-State, Special Events, and Domestic Incidents. The Events and Incidents capability includes the following features: editable, state-Specific Steady-State facility information including consequence, vulnerability, threat, and resilience indices for state/local users to monitor and update; editable, Special Events that can cross-reference Steady-State facility information and propose mitigated vulnerability and mitigated risk indices for state/local users to monitor and update pre-event; and editable, Domestic Incident events that can cross-reference Steady-State facility information. Facility operability, critical infrastructure needs, Requests for Action/ Requests for Information (RFA/RFI), and reports can be generated, monitored, and updated as the incident progresses; and a searchable, customizable facility list.

Infrastructure Data Call Application (IDCA) - IDCA is web-based data collection tool that was designed to collect annual submissions to the National Critical Infrastructure Prioritization Program (NCIPP) managed by the National Risk Management Center (NRMC). Submissions can be entered by state and territorial Homeland Security Advisors (HSA), federal Sector-Specific Agencies (SSA), and Protective Security Advisors (PSA).

Infrastructure Survey Dashboard – The Infrastructure Survey Dashboard allows for users to search and view interactive facility dashboards from the system. The web-based dashboards are used to convey, track, manage and graphically display information collected by the PSAs or through incident or suspicious activity reporting.

Map View - The Map View enables users to visualize critical infrastructure resources in a geospatial context. The Map Viewer provides users with the ability to drill down and view numerous data layers for specific states, counties, or cities. These layers include static layers, such as facilities-by-sector, daytime population, or street-view pictures; and dynamic layers, such as

current wildfire or weather elements. These geographically accurate presentations provide a wealth of visual information, affording IP mission partners with an in-depth look at an area's operational situation. The Chemical Facility Anti-Terrorism Standards (CFATS) system has an integration into the Map View as a Data Layer used to display CFATS facilities and allow users to view and download Top-screen and Tiering Report information.

CISA Central WebEOC – The CISA Central WebEOC is a multi-purpose web-based application engineered to assist and support CISA Central Duty Officers and the broader CISA Central end-user community in managing information related to critical infrastructure. WebEOC is an incident management system with wide-ranging capabilities including: documenting and cataloging data in a searchable enterprise-level database, managing information workflows, automatically generating finished reports, and creating a timeline of events that are shared among WebEOC users. Furthermore, WebEOC provides users with 24/7 situational awareness through the capturing and dissemination of timely, relevant, and actionable information.

The CISA Central WebEOC also supports the CISA Central watch analysts and the broader ISD community to manage information and incidents related to critical infrastructure. This system manages information workflows for several CISA Central-created products including Data Capture, Request for Information (RFI) responses, and Current Situation Reports (CSR). WebEOC automatically generates PDF reports from internal records that are distributed to stakeholders. WebEOC also functions as a data management tool by recording and cataloging RFIs, National Response Center (NRC) emails, watch operations log (Data Capture) and all CISA Central reports and products. These records create a timeline of events that is shared among WebEOC users.

CISA Situational Awareness Tool – The CISA Situational Awareness Tool (SAT) provides users the ability to create incidents and fuse multiple datasets together to rapidly aggregate information, such as an incidents potential impact on critical infrastructure or population, and to visualize and disseminate this information to other users, key decision makers and stakeholders.

Stakeholder Risk Assessment and Mitigation (SRAM) Portal - The SRAM Portal provides a central repository of contact information, calendar functions, assessment questions, assessment reports/dashboards, and automated workflows of assessment logistics and processes. The SRAM Portal is tailored specifically for the collection of SRAM evaluation data capture and tracking needs.

Surveys and Assessments - The Surveys and Assessments Tool (formerly Infrastructure Survey Tool) is a web-based tool used to facilitate data collection and analysis. It was designed as a multi-use tool to be used during PSA and SLTT visits to critical infrastructure sites. Surveys come in three sizes depending on amount of time available to perform the survey – Rapid (shortest), Standard, and Enhanced (longest). The application produces a dashboard for the owner

and operator to view their assessment information and manipulate it to identify measures that can be taken to increase their security and resilience scores.

Information Sharing and Training Tools

Digital Library - The Digital Library provides access and a method to search for key research and reports related to critical infrastructure. With the Digital Library, a user can access thousands of documents related to critical infrastructure ranging from facility assessments to sector specific standards. Documents come from the information within the CISA Gateway system. Documents are also pulled from several open source sites. Users also have the ability to add relevant documents to the library via a link in the Digital Library. Recommended documents will be sent to the Digital Library librarian using the system's content management system for approval before upload.

Infrastructure Protection Report Series (IPRS) - IPRS is a comprehensive series of reports developed by PSCD to increase awareness of the infrastructure protection mission and build a baseline of security knowledge throughout the Nation to help deter, detect, defend, respond, and recover from a terrorist attack or natural or man-made disaster. The IPRS focuses on infrastructure characteristics and common vulnerabilities (CV), potential indicators of terrorist activity (PI), and associated protective measures (PM) and are referred to as CV/PI/PM Reports.

Administrative, Management, and Reporting Capabilities

Calendar - The Calendar is used by assessors to track upcoming surveys and assessments. This read-only capability displays for official use only (FOUO) data only and is populated by the scheduling information collected in the Surveys and Assessments area. The Calendar displays the scheduling information for asset visits from the IST/Surveys and Assessments Tool. This supports situational awareness for ISD personnel.

CISA Gateway Landing Page – The Landing Page includes information available to users about the latest updates to the site, as well as the option to personally configure the landing page allowing users to quickly access their data from each CISA Gateway application.

CISA Gateway User Management (Manage Users) – The Manage Users tool allows System Administrators to manage the users of the system. This management includes approving or rejecting new user's requests, approving or rejecting access requests, editing user's information, and editing user access.

CISA Gateway User Registration – The User Registration tool is used during initial user submission for accounts on the CISA Gateway system. Users fill out the information included in

the User Registration tool which allows the System Administrators to validate, approve, deny, request more information, and set up accounts for users on the CISA Gateway system.

Cyber Information Sharing and Collaboration Program (CISCP) Tracker - The CISCP Tracker provides a means of tracking the creation and approval process of CISCP Cooperative Research and Development Agreements (CRADA) and managing relationships with CISCP stakeholders by serving as a repository for organization information, points-of-contact and meeting notes. CRADAs are legal documents that are established between the federal government and commercial entities for the purposes of creating a collective environment for the research and development of technology.

Data Taxonomy – The Data Taxonomy facilitates a common understanding of infrastructure terminology within the infrastructure protection community. It does this by categorizing infrastructure assets and establishes a common language for all to use. The IDT is structured into five levels of detail, although not all assets require all five levels. In descending order, these levels are sector, subsector, segment, sub-segment, and asset type.

Metrics – the Metrics application allows ISD and IAA users to view or print reports from the CISA Gateway user survey information that was voluntarily submitted by federal users.

Personnel Activity Application (PAA) - PAA allows the user to capture contact information, activities, and program information and produce reports on all areas. The application also has a standard workflow and template for after action reports. The application is role-based and provides different read/write options for each role. One role has the ability to view his/her own inputs and the other role allows supervisors to review and pull metrics on all employee activities.

Protected Critical Infrastructure Information Management System (PCIIMS) - PCIIMS is a suite of information technology applications and the means by which Critical Infrastructure Information submitted from the private sector is received, validated, protected, and catalogued as Protected Critical Infrastructure Information. PCIIMS also facilitates the training, registration, and management of all PCII Authorized Users.

Trip Tracker - The Trip Tracker is used for scheduling trips and visits to facilities for various type of assessments. Users include DHS Headquarters and supporting field personnel. The application provides a workflow that uses a consistent method for scheduling facility visits across PSAs with notifications when changes are made to a visit. The application allows the user to look up available personnel and assign them to the visits. The Trip Tracker produces reports of all scheduled visits and shares the visit dates and assignments with the Weekly Activity Report application.