CISA GATEWAY DATA PROTECTIONS

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) Gateway is a system of systems providing a single interface through which CISA mission partners can access a large range of integrated critical infrastructure information and tools. This enables users to collect, manage, protect, and share critical infrastructure data through a single platform, resulting in more effective data analysis. The system maximizes the availability of data for cross-government sharing, offering advanced data analysis, and planning capabilities in support of day-to-day operations, enhancing the protection and resilience of critical infrastructure, supporting special events and exercises planning, and incident response and recovery. The key behind this system is the sensitive and unique data which it houses. CISA is committed to ensuring that all data gathered and shared is legally and technically protected from disclosure to maintain its confidentiality and integrity. This fact sheet covers the technical protections within the CISA Gateway.

SECURITY STANDARDS

RISK MANAGEMENT AND CYBERSECURITY GOVERNANCE

CISA adheres to the latest version of the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-37r2 Risk Management Framework for assessing any systems it maintains.

CISA is moving to an ongoing review and authorization cycle versus the three-year authority to operate method for authorizing systems, allowing for continuous monitoring and adjustment to the security posture and boundary of the system. This structure employs a constant analysis and assessment of the security architecture and associated controls to ensure the entire system remains aligned with the most current security standards. The process for authorization includes comprehensive system scanning, penetration testing (red teaming), and other mechanisms. A secure code review is conducted as part of the accreditation process.

The CISA Gateway complies with the Department of Homeland Security (DHS) Sensitive Systems Policy Directive 4300A v13.1 and associated CISA and federal government directives that govern the policies and procedures for all IT systems deployed within DHS. The system meets strict security standards to ensure all operating system and software application patches are constantly evaluated, applied, and maintained. CISA maintains a standard of addressing all critical and high rated vulnerabilities within a 15-day window and all other vulnerabilities within a 30-day window.

CISA and DHS utilize the Defense Information Systems Agency Security Technical Implementation Guides and NIST SP standards for secure configurations of its systems.

SYSTEM ARCHITECTURE

The CISA Gateway resides in a cloud-based architecture that enhances the security and resiliency of the system by leveraging a Federal Risk and Authorization Management Program (FedRAMP) High certified Government Cloud (GovCloud) for hosting its environment. The system maintains a defense-in-depth architecture utilizing layered security throughout.

Account Management | **Identification and Authentication** | **Principle of Least Functionality**

The CISA Gateway employs multiple industry-standard best practices for the protection of stored data. By leveraging role-based access and least-privilege principles for all aspects of the system and data, the system ensures and validates need-to-know prior to granting system access. User identities are authenticated leveraging phishing-resistant multifactor authentication (MFA) mechanisms. Privileges and access are assessed on an ongoing basis for all users.

DATA PROTECTION

All internal and external connections in and out of the system are fully monitored and controlled internally by the CISA Gateway Operations and Security teams and externally by the DHS Security Operation Center, traversing the DHS Trusted Internet Connection. Any intersystem connection for dynamic feeds in and out of the system are protected with encrypted virtual private network tunnels, encrypted Transport Layer Security sessions, or secured application programming interfaces with authentication mechanisms employed.

SECURITY MONITORING

All files uploaded into the system are scanned upon entry and on an ongoing basis for virus/malware/etc. Within the layered architecture, web application firewalls, Intrusion Detection and Prevention Systems, and other best practices are implemented. The system ensures all Data-in-Transit and Data-at-Rest are secured using Federal Information Processing Standards 140-2 or enhanced encryption mechanisms.

HOST SECURITY

While we have initial Continuous Diagnostics and Mitigation (CDM) capabilities deployed within the system, the CISA Gateway Program Office is deploying the entire suite of the CISA CDM/Virtual Enterprise Network Operations Manager tools to further supplement the following areas: Asset Discovery and Scanning, User Management, Incident Response, and Data Protection.

The CISA Gateway maintains backups of all data and performs National Security Agency compliant data sanitization mechanisms. The Cloud architecture provides superior availability and seamless failover between the redundant systems allowing for significantly reduced user impact if an outage were to occur. The Cloud provides the ability to scale resources up or down to support surges in user demand during critical infrastructure incidents resulting from weather or man-made events.

RESOURCES

If you would like to learn how the CISA Gateway can support your organization's homeland security efforts, to inquire about eligibility for accessing the CISA Gateway, or if you would like to establish access to the system, please contact the CISA Gateway Program Office at CISA-Gateway@mail.cisa.dhs.gov.

To learn more regarding the CISA Gateway, visit cisa.gov/cisa-gateway.