# Modernizing Cybersecurity Programs

*November 16, 2020*

Fiscal Year 2020 Report to Congress

Homeland Security

*Cybersecurity and Infrastructure Security Agency*

# Message from the Director

November 16, 2020

I am pleased to provide the following report, "Modernizing Cybersecurity Programs," which has been prepared by the Cybersecurity and Infrastructure Security Agency (CISA).

This report was compiled pursuant to direction in the Joint Explanatory Statement, House Report 116-180, and Senate Report 116-125, all accompanying the Fiscal Year (FY) 2020 Department of Homeland Security (DHS) Appropriations Act (P.L. 116-93).

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable Lucille Roybal-Allard
Chairwoman, House Appropriations Subcommittee on Homeland Security

The Honorable Chuck Fleischmann
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Shelley Moore Capito
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jon Tester
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to CISA Legislative Affairs at (202) 819-2612.

Sincerely,

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency

# Executive Summary

CISA is leading the civilian governmentwide effort to improve cybersecurity operations, including agencies' visibility into their networks (in both cloud and on-premises environments) to detect and respond to cybersecurity incidents effectively.

CISA is applying experiences gained from initial research and pilot efforts to improve its National Cybersecurity Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM) capabilities. CISA is working closely with the Federal Risk and Authorization Management Program and other entities within the U.S. General Services Administration to ensure that when contracting with cloud providers, agencies can use governmentwide security clauses to ensure better data protections. To this end, CISA is identifying new capabilities and strategies to protect government data in the cloud by both cloud tenants (agencies) and the cloud service providers (CSP) or by cloud security access brokers (CSAB) that serve as sources for agencies' hardware, software, infrastructure, and security services.

NCPS is an integrated system-of-systems that provides intrusion detection and prevention capabilities, advanced analytics, and information-sharing mechanisms that mitigate cyber threats to federal civilian networks and augment their internal cyber capabilities. The NCPS suite of capabilities enables CISA to enhance the security of federal agencies against advanced cyber threats. NCPS capabilities are evolving to support the increasing adoption of cloud services. Although traditional network intrusion detection and prevention capabilities remain useful, NCPS must evolve. The NCPS program is working with agencies and their CSPs and CSABs to identify and pilot solutions for their evolving architecture. The combination of CDM and NCPS capabilities in the cloud are expected to provide agencies as well as CISA with the capabilities and data necessary to meet this mission.

Over the last several years, CDM has expanded its core cybersecurity capability offerings through the Dynamic and Evolving Federal Enterprise Network Defense acquisition program to provide greater flexibility to agencies for implementing the CDM requirements. The CDM program has defined how its capabilities can be deployed to the cloud including completion of a pilot with the Small Business Administration, which has moved a significant portion of its data processing to the cloud.

CISA is committed to consistent and continuous improvement of security operations at federal civilian agencies and is adapting the current capabilities of CDM and NCPS while also planning for long-term capability enhancements. CISA also is working with the Office of Management and Budget to evaluate the current state of cybersecurity operations across the Federal Government and to identify and standardize the core security operations centers (SOC) capabilities offerings in the agencies. Based on their specific needs and availability of internal capacity and expertise, agencies eventually will be able to decide whether to supplement their existing capabilities with individual, third-party-provided SOC services, or to migrate their SOC operations to a SOC-as-a-Service model.

# Modernizing Cybersecurity Programs

## Table of Contents


I. Legislative Language ..... 1

II. Background ..... 2

III. Discussion ..... 4

A. Continuous Diagnostics and Mitigation Program ..... 4
Keeping CDM Operationally Effective ..... 4
Continuing pilot programs that extend incident detection and prevention to federal endpoints ..... 5
A long-term, strategic vision ..... 5

B. National Cybersecurity Protection System Program ..... 6
NCPS Modernization ..... 8
Modernizing the EINSTEIN Sensor Suite ..... 8
How Agency Cloud Adoption Affects NCPS ..... 8
NCPS Cloud Telemetry Cycle ..... 9
Benefits of Sharing Cloud Security Data With CISA ..... 10
NCPS Roles, Responsibilities, and Cloud Operations ..... 10
CISA Cloud Data Aggregation ..... 12
Cloud Log Aggregation Warehouse Overview ..... 12
CLAW Distribution ..... 12
CISA Analysis of Agency Data ..... 13
Modernizing the NCPS Core Infrastructure and Capabilities ..... 14
NCPS Infrastructure Modernization ..... 14
NCPS Application Environment ..... 14

IV. Conclusion ..... 16

Appendix - Abbreviations ..... 17

# I. Legislative Language

This document was compiled pursuant to language set forth in the Joint Explanatory Statement, House Report 116-180, and Senate Report 116-125, all accompanying the Fiscal Year (FY) 2020 Department of Homeland Security (DHS) Appropriations Act (P.L. 116-93).

The Joint Explanatory Statement states:

> CISA is directed to provide a report not later than 180 days after the date of enactment of this Act detailing how CISA will modernize CDM and National Cybersecurity Protection System (NCPS), including EINSTEIN, to ensure they remain operationally effective given changing trends in technology, the federal workforce, threats, and vulnerabilities. The report shall address the requirements described in the House and Senate Reports.

House Report 116-180 states:

> The Committee is concerned with the security implications of an increasingly modern federal workforce, which includes more remote employees, enhanced mobility, and an increased focus on cloud technologies. CISA is directed to brief the Committee not later than 180 days after the date of enactment of this Act on a detailed plan to modernize CDM and NCPS to ensure they remain operationally effective given changing trends in technology, the federal workforce, threats, and vulnerabilities. The briefing shall include: (1) a long-term, strategic vision for the program to ensure that CDM and NCPS capabilities continue to develop and evolve in an agile manner to address contemporary technology use and vulnerabilities and combat emerging cybersecurity threats; (2) an assessment of whether emerging private sector technologies that focus on securing endpoints could integrate with existing program capabilities to enhance the overall effectiveness of CDM and NCPS; and (3) preliminary results from all CDM and NCPS-related pilot programs.

Senate Report 116-125 states:

> CISA is directed to provide a report no later than 180 days after the date of enactment of this act detailing how CISA will modernize the NCPS, including EINSTEIN. The report should include how EINSTEIN will remain relevant given changing trends in technology and the Federal workforce and provide a strategic outlook for how CISA plans to evolve EINSTEIN over the next 5 years. The report should address emerging technologies, including those which focus on securing endpoints, and how emerging technologies could be integrated with existing program capabilities to enhance EINSTEIN's overall effectiveness.

# II. Background

The Cybersecurity and Infrastructure Security Agency (CISA) is leading the civilian governmentwide effort to improve federal cybersecurity operations, including agencies' visibility into their networks (in both cloud and on-site environments) to detect and respond to cybersecurity incidents effectively. CISA is ensuring that its cyber programs remain operationally effective given the changing trends in technology, the federal workforce, threats, and vulnerabilities. Further, experience with increased telework since March 2020 has caused CISA's major cybersecurity programs (NCPS and Continuous Diagnostics and Mitigation [CDM]) to focus their efforts further on information technology (IT) modernization, including the interim telework guidance released in April.[1]

NCPS is an integrated system-of-systems that provides intrusion detection and prevention capabilities, advanced analytics, and information-sharing mechanisms that mitigate cyber threats to federal civilian networks. These capabilities provide a technological foundation that enables CISA to secure federal agencies against advanced cyber threats.

NCPS capabilities are evolving to support the increasing adoption of cloud services. The legacy intrusion detection capabilities were designed to support a perimeter-based network architecture. Although traditional network intrusion detection and prevention capabilities remain useful, NCPS must evolve its capabilities, such as being able to ingest cloud security data from commercial cloud vendors. The NCPS program is working with agencies and cloud service providers (CSP) to identify and pilot solutions that support the evolving architecture. The combination of CDM and NCPS capabilities in the cloud are expected to provide agencies as well as CISA with the capabilities and data necessary to meet this mission.

The CDM program bolsters agency cyber defenses and enhances the security posture of the Federal Government by providing federal agencies with capabilities to monitor risks to their networks in near real-time. This increased situational awareness allows agencies to prioritize actions to mitigate or accept cybersecurity risks based on an understanding of the potential impacts to their mission. The CDM program accomplishes this by deploying commercial off-the-shelf tools on agency networks that provide enterprisewide visibility of what assets, users, and activities are on their networks. This actionable information allows agencies to monitor, defend, and respond rapidly to cyber incidents. CDM capabilities are organized into five key program areas: deployment of agency and federal dashboards, asset management, identity and access management, network security management, and data protection management.

CISA's cybersecurity programs directly support the following federal goals and mandates:

- *Report to the President on Federal Information Technology (IT) Modernization* as provided under Executive Order 13800 (May 11, 2017);

[1] See CISA, Trusted Internet Connections 3.0, Interim Telework Guidance (April 8, 2020), available at: https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf.

- President's Management Agenda, which includes an IT priority of reducing cybersecurity risks to the federal mission by leveraging current commercial capabilities and by implementing cutting-edge cybersecurity capabilities;
- Federal Information Security Modernization Act of 2014, which authorizes DHS to deploy technology to assist agencies in continuously diagnosing and mitigating cyber threats and vulnerabilities;
- Office of Management and Budget (OMB) Circular No. A-130 (2016 revision), *Managing Information as a Strategic Resource*, which directs federal civilian agencies to develop and implement information security continuous monitoring strategies; and
- OMB Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, which provides guidance to agencies on strengthening CDM capabilities.

To ensure that both programs continue to evolve with a rapidly changing cyber environment, CISA is committed to continuous program improvements. CISA has established the .gov Cyber Architecture Review (.govCAR) methodology to conduct threat-based assessment of cyber capabilities. This approach looks at the target architecture the way that an adversary does and directly identifies where mitigations can be applied for the best defense against all phases of a cyber-attack. The .govCAR methodology parallels the Department of Defense's project known as the Department of Defense Cybersecurity Analysis and Review, which introduced the concept of a threat-based, end-to-end analysis of large, enterprise cybersecurity architectures. It is used to provide direction and justification for CISA's cybersecurity programs in that any .govCAR recommendations regarding the efficacy of certain technologies is considered during investment review.

This report provides insight into how CISA is ensuring that its cyber programs remain operationally effective given the changing trends in technology, the federal workforce, threats, and vulnerabilities.

# III. Discussion

## A. Continuous Diagnostics and Mitigation Program

**Keeping CDM Operationally Effective**

CISA is focused on ensuring that CDM capabilities remain operationally effective. From the contracts perspective, CDM is using its Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) contract vehicle, offered under the U.S. General Services Administration's Alliant/Alliant II offering, which includes various improvements over CDM's initial contract vehicles. The DEFEND contracts offer higher ceilings, longer periods of performance, and all CDM capabilities offering much more flexibility to agencies to match their requirements.

Further, in May 2020, CDM awarded its next-generation shared services platform to ensure that the smaller, non-Chief Financial Officers Act of 1990 (P.L. 101–576) (CFO Act) agencies can leverage CDM capabilities in a cost-efficient manner, enabling them to manage their assets, identities and accounts, and network services, and to protect their data on par with the CDM tools and resources available to the much larger CFO Act agencies. Today, 36 non-CFO Act agencies are operational on the existing shared services platform.

Recognizing that the federal workforce is highly mobile, CDM is adding mobile asset management capabilities in the next year. CDM will interface with agencies' enterprise mobility management systems to align mobile asset reporting better. CDM also plans on providing mobile threat capabilities to reinforce the security of agencies' enterprise mobility management systems and mobile devices.

Through CDM, CISA also is providing data protection management capabilities to agencies, which offer strong protection to the sensitive data on some of the Federal Government's most critical systems, termed high-value assets (HVA). HVAs include networks that are essential to the agency functions, are designated as essential to maintaining the security and resiliency of the federal civilian .gov enterprise, or both. With the data protection management capability, CISA is working with agencies and industry to strengthen the data protections of the Federal Government's HVAs. These tools provide the HVAs with advanced threat-detection capabilities.

CDM also is transitioning the agency and federal dashboard ecosystem in 2020, offering higher performance, more flexibility, and greater scalability. The migration to a robust big data platform will evolve into significant advances over time, as the CDM program adds capabilities and functionality to promote situational awareness for threat-based defense. These capabilities will include enhanced vulnerability prioritization, threat-based data enrichment, incident response reporting and orchestrated workflow, integration with additional NCPS capabilities, data analytics, and machine learning. The new dashboard will ingest data into a common schema, which will make analytics sharing across agencies or their bureaus much easier.

In addition, CISA will be evaluating the efficacy of incorporating "break and inspect" capabilities into the CDM architecture to address challenges associated with inspecting and securing encrypted network traffic at scale without degrading performance. The CDM program is working with NCPS and trusted internet connection (TIC) programs to evaluate "break and inspect" opportunities against the risks of decrypting sensitive government data. Concerns regarding the potential increase in attack surface that this methodology might introduce to both agencies and DHS must be addressed and mitigated.

**Continuing pilot programs that extend incident detection and prevention to federal endpoints**

To extend CISA's incident detection and prevention capabilities to federal endpoints, CISA's CDM program and Threat Hunting subdivision have been working since 2019 to pilot new efforts. CISA is working with the respective agencies to identify appropriate endpoints, existing tools, and other details for pilots that began in the fourth quarter of FY 2020.

The pilots will use existing host-based sensors to provide real-time cyber information to agency and CISA cyber analysts. The pilots will allow the teams to consider the value of the sensor data received and to gain early experience on whether such an approach merits more widespread consideration across the federal network enterprise.

**A long-term, strategic vision**

CISA's long-term strategy has been informed by the significant sudden growth in teleworking by the Federal Government over the last few months. While the agency was keenly aware already of the need for agility and flexibility for its cyber programs, that need was reinforced fully in mid-March when the entire Federal Government shifted to telework environments. In response, CISA continued to support its federal (and other stakeholders) albeit with a new emphasis on remote meetings, video calls, multi-platform collaboration tools, etc. CISA is leveraging this digital transformation and sharpening its focus on new work modes, new tools, future products, and evolving workforce efficiencies.

Additionally, CISA has responded by surging additional CDM resources to agencies urgently requiring support for accelerated moves to the cloud, strengthening asset and identity management, and other activities.

The ongoing federal transition from on-premises architectures to cloud-computing modes creates a fundamental shift for agency cybersecurity. Because of the complex and disparate nature of cloud computing, this transition affects the location, means, and methods of protecting agency data. When agencies adopt a data-centric security approach, in which data itself is conceptualized as an asset, it necessitates an evolution in the ways by which agencies protect data regardless of its location. CISA's CDM capabilities are adapting to align with this new design approach.

Ensuring that CDM's capabilities and outcomes are achieved fully relies in part on expanded pilots and sharing industry best practices and lessons learned with the agencies. Following are examples of cloud initiatives that CDM has completed or has underway.

***CDM Cloud Guidance Document*:** Version 2 of the CDM Cloud Guidance Document will be released in the fourth quarter of 2020. It will focus on threats to cloud ecosystems and, where possible, will identify the data flows and sources available today that will help agencies to gain visibility into their risks. This will include, for example, a focus on Identity, Credential, and Access Management, which will allow agencies to focus resources on strengthening cloud access to data assets. The document will outline fundamental principles, challenges, and recommended practices for protecting identity assets and infrastructure in cloud environments.

Version 2 also will incorporate the threat-based .govCAR methodology, which assesses vulnerabilities in an architecture the way that an adversary may, and then directly identifies where mitigations can be applied for the best defense against all phases of a cyberattack.

***CDM DEFEND Cloud Activities*:** Experience and best practices gained from initial release of the cloud discovery activities under the DEFEND-C Task Order will be used to refine future cloud activities at other federal agencies.

***CDM Cloud Pilot Project*:** As noted earlier, CDM partnered with the Small Business Administration to conduct a pilot on using cloud-native tools to support CDM requirements. The pilot report, released in May 2020, identifies successes and pinpoints potential capability gaps related to functional and operational requirements and dashboard capabilities. The report will inform the future direction of CDM with respect to cloud efforts.

***CDM Cloud Lab*:** CDM is taking a threat-based approach to achieve visibility in the cloud ecosystems. Cloud architectures present various challenges to CDM's collection of actionable and relevant information such as what data helps agencies to understand their cloud security risks, how to organize this information into meaningful groupings that then can be analyzed and risk scored, and to identify who is accessing these cloud architectures and what they are doing once they have been granted access. This approach identifies CDM capabilities that will be prioritized under cloud activities and the common data sources that might exist in various cloud technology platforms.

## B. National Cybersecurity Protection System Program

NCPS is an integrated system-of-systems that provides intrusion detection and prevention capabilities, advanced analytics, and information-sharing capabilities that together provide to both CISA and federal agencies the ability to mitigate cyber threats. The NCPS capabilities, and specifically the EINSTEIN intrusion detection and prevention sensor suite (EINSTEIN 1[E1]/ EINSTEIN 2[E2]/EINSTEIN 3 Accelerated [E3A]), are capabilities that support a defense-in-depth approach in support of CISA's federal network defense mission.

- ***Intrusion Detection*:** NCPS's intrusion detection capabilities such as E1 (Netflow) and E2 (Intrusion Detection) alert CISA and federal agencies to malicious activity within

their networks. Using a signature-based sensor grid, the system monitors network traffic for malicious activity traveling to and from federal networks. Signatures are specific patterns of network traffic that can be used to identify malicious activity and are derived from numerous sources, such as commercial cyber threat information, incidents reported to CISA, information from CISA's partners, or in-depth analysis. Intrusion detection provides federal agencies with near real-time detection and notification capabilities. In 2018, NCPS operationalized a nonsignature-based detection system that enhances CISA's intrusion detection capabilities to include functionality that detects deviations from normal network behavior baselines.

- ***Intrusion Prevention*:** NCPS's intrusion prevention capabilities are delivered through the E3A portion of the program and are capable of automatically detecting and responding to cyber threats in near real-time. Deployed directly by the internet service providers (ISP) that provide service to the Federal Government, the system leverages classified and unclassified indicators to block known malicious traffic before it reaches agency networks. This allows for enhanced cybersecurity analysis, situational awareness, and security response, providing for active network defense and the ability to limit malicious activities from penetrating federal networks.

- ***Analytics*:** CISA cyber analysts compile and analyze information about current and potential cybersecurity threats. This information is shared, consistent with statutory limits on how NCPS information can be retained, used, and disclosed[2], with CISA's public- and private-sector partners and the public. NCPS's analytics capabilities include a range of technologies, including Security and Event Management, Packet Capture, Enhanced Analytical Database and Flow Visualization, and Advanced Malware Analysis.

- ***Information Sharing*:** CISA shares much of this analysis, along with additional computer network security information, with its public- and private-sector partners rapidly and in a secure environment. NCPS-derived analysis also is shared through commercial data feeds, internally generated analytic products, analytics tools, threat indicators and warnings, and real-time incident and continuous monitoring data. These services provide CISA cyber analysts and their cyber partners with a common operating picture of the threat landscape. All information sharing is accomplished consistent with statutory limits on how NCPS information can be retained, used, and disclosed.

- ***Core Infrastructure*:** NCPS Core Infrastructure capabilities comprise the backend data storage and processing environment, known as the Mission Operational Environment, including network devices, storage devices, database services, application hosting services, and security controls. These capabilities relate to the command and control of the EINSTEIN sensors and services. This capability also includes the Analytics and Information Sharing environment for CISA operators and analysts.

[2] *See* 6 U.S.C. § 663(c)(3).

## NCPS Modernization

The NCPS program is evolving to ensure that security information from federal agencies' cloud-based traffic can be captured and analyzed for CISA cyber analysts to provide situational awareness and support to the agencies. This is occurring primarily through the modernization of NCPS EINSTEIN capabilities. In addition to developing the EINSTEIN cloud-based architecture to collect and analyze agency cloud security data, NCPS also is modernizing its backend analytic, information- sharing, and core infrastructure areas to improve CISA's ability to collect, process, analyze, and share cyber data with its stakeholders through Federal Risk and Authorization Management Program-authorized commercial and government cloud services. This NCPS modernization effort will reduce capital infrastructure investments at DHS data centers and will allow the NCPS program to be more agile in meeting evolving cyber threats and mission needs. Lastly, the increased utilization of commercial cloud capabilities across NCPS will improve the scalability, availability, and reliability of the infrastructure, capabilities, and services for CISA and federal agencies.

## Modernizing the EINSTEIN Sensor Suite

As agencies move more of their applications and services to the cloud, the NCPS program is evolving to ensure that security information about cloud-based traffic can be captured and analyzed and that CISA cyber analysts can continue to provide situational awareness and support to the agencies. Traditionally, TIC access points (either MTIPS gateways or agency-managed TIC access points[3]) contain EINSTEIN[4] sensors, so when an agency participates in the TIC program, it also automatically utilizes the capabilities of the NCPS program. As such, agencies traditionally have been able to fulfill NCPS requirements simply by complying with the TIC program. However, in 2019, OMB issued an updated TIC policy, OMB Memorandum M-19-26[5], which does not require TIC access points to be embedded in all TIC use cases. Many of these new TIC use cases describe cloud services. In these use cases, network traffic between an agency and a CSP does not pass through an EINSTEIN sensor.

As agencies and CISA adopt cloud environments and conform to the new TIC use cases, they will continue to share telemetry and security insights.

## How Agency Cloud Adoption Affects NCPS

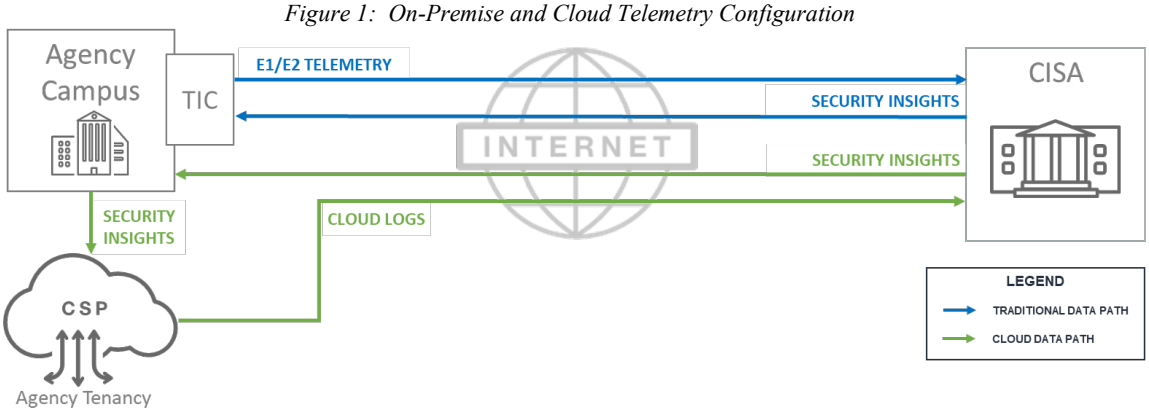
As part of their IT modernization efforts, many agencies are utilizing commercial cloud products and adopting cloud email, collaboration, and software tools. Many agencies are using multiple CSPs in order to meet their mission needs and are utilizing all three cloud service models: Software as a Service (SaaS), Platform as a Service, and Infrastructure as a Service.[6] When an agency creates a tenancy within a CSP, traffic between that CSP and the agency no longer may pass through a TIC access point or an NCPS sensor.

---

[3] https://www.cisa.gov/trusted-internet-connections
[4] https://www.cisa.gov/einstein
[5] https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf
[6] Email as a Service is a sub-type of SaaS.

Figure 1 depicts the relationship between an agency's CSP tenancy and CISA. In this diagram, an agency still has some of its network traffic traversing the traditional TIC access point, but network traffic to or within one or more CSPs does not pass through the TIC access point. The top data flow paths show the traditional flow of E1/E2 telemetry from the agency to CISA and the flow of security insight from CISA to the agency. The bottom data flow paths show the new data flows between the agency, the CSP, and CISA.

*Figure 1: On-Premise and Cloud Telemetry Configuration*



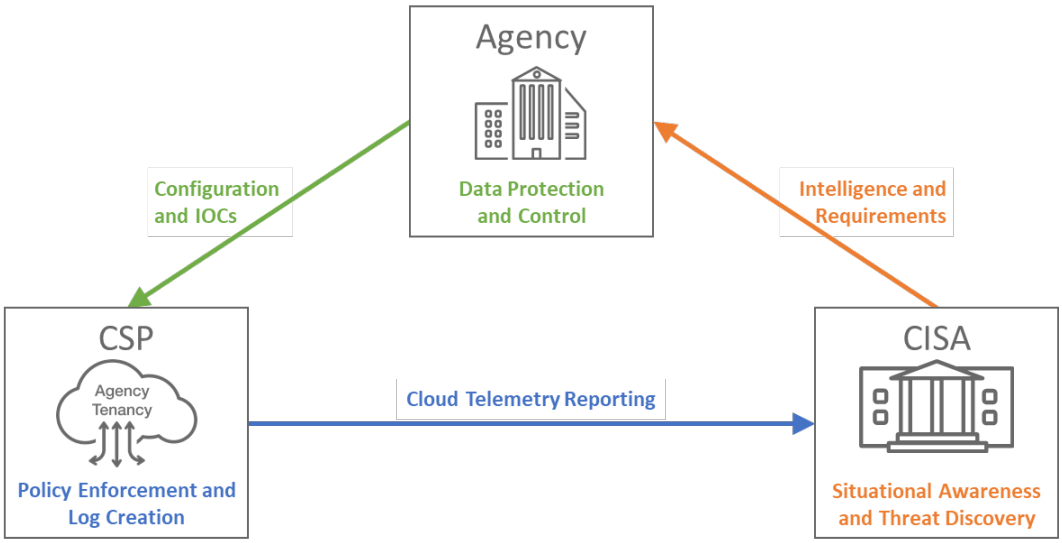

Because there is a wide range of CSPs and tenant-controlled security tools, there will be new data formats for telemetry (other than traditional network flows) and potential new formats for security insights for NCPS in the cloud.

**NCPS Cloud Telemetry Cycle**

In order to realize fully the collection of cloud data to fulfill NCPS requirements, there is a need to define the NCPS cloud telemetry cycle, as depicted in Figure 2. Each of the entities in the cycle has unique roles and responsibilities:

- CISA sends intelligence and requirements to agencies (as depicted by the orange arrow).
- An agency is responsible for protecting its data, both on-premise and in the cloud, and the agency leverages intelligence and requirements to set configurations and indicators of compromise (IOC) in its cloud instances (as depicted by the green arrow).
- CSP monitoring and policy enforcement agents generate logs or security data and send them to CISA as cloud telemetry (as depicted by the blue arrow).
- CISA uses the cloud security data to inform situational awareness and threat discovery, resulting in new cyber threat intelligence sent to agencies (as depicted by the orange arrow).

*Figure 2: NCPS Cloud Telemetry Cycle*




**Benefits of Sharing Cloud Security Data With CISA**

There are several benefits associated with sharing cloud security data with CISA:

1. Expanding NCPS to include agency cloud data provides CISA with the ability to gain situational awareness of threats and threat actors across the federal networks' domain, including on federal agencies' cloud communications. As a result, CISA can respond proactively to and mitigate cloud-based attacks against federal networks.
2. The inclusion of agency cloud telemetry extends CISA's security visibility and protection perimeter to include cloud-hosted software interactions and third-party services. This increased visibility informs and enhances incident response capabilities and federal cloud security posture. All agencies and CISA benefit from that extended visibility.
3. Additional cloud telemetry provides CISA with the ability to aggregate and correlate threat data generated and consumed in the cloud to aid in the timely discovery of security vulnerabilities and attack campaigns facing federal network cloud infrastructure.
4. Data gathered from the cloud network flow and cloud security data provide CISA with additional cyber threat intelligence and information to predict the changing security landscapes of both on-premise and cloud infrastructure, as well as to plan, execute, and manage security countermeasures accurately on the federal scale.
5. EINSTEIN in the cloud provides a centralized model for log aggregation and analysis of a broad data set from federal cloud deployments, which results in a greater risk reduction for individual agencies as well as better availability of IOCs to Federal Government information resources.

**NCPS Roles, Responsibilities, and Cloud Operations**

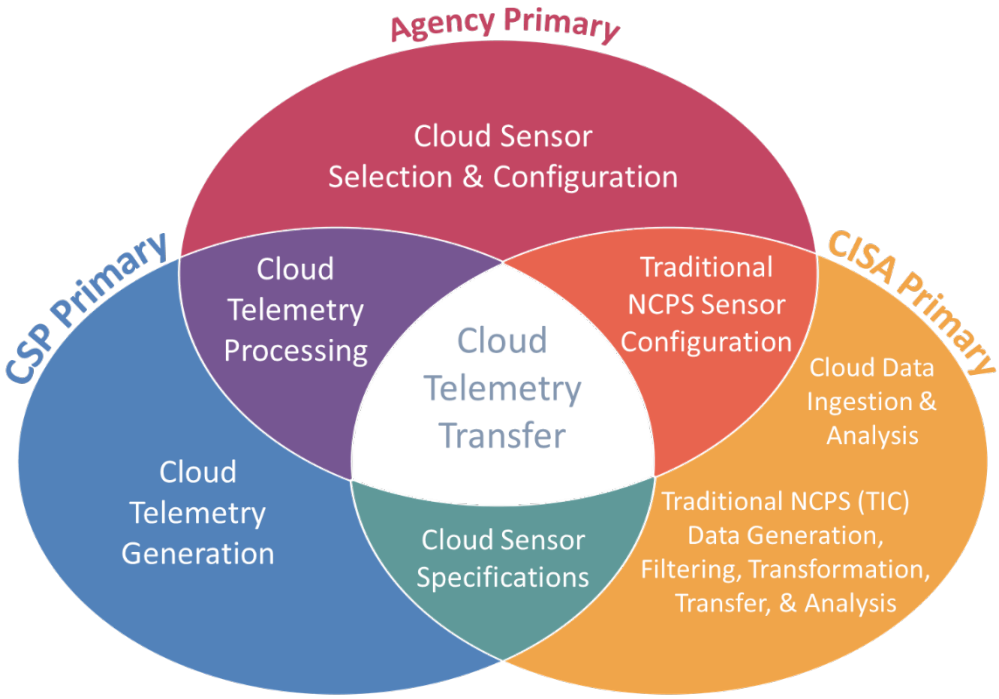
Transitioning to the cloud introduces new roles, actors, and procedures (e.g., an autonomous CSP, absence of TIC, third-party cloud monitoring tools, etc.) and the existing system for NCPS security insights (includes cyber threat indicators and/or signatures) transmission needs to be

adapted. Specifically, in existing EINSTEIN on-premise deployments, security insights in EINSTEIN are forwarded from CISA to the TIC access point via the EINSTEIN sensor platform. However, when agencies utilize CSPs, there is the introduction of a new telemetry exchange. EINSTEIN security insights continue to be transmitted from CISA to the TIC access points, but agencies also need to "pull" EINSTEIN security insights from CISA and to transmit those security insights to their agency tenant protections hosted by CSPs.

CISA's cloud presence for collecting and analyzing EINSTEIN information is called the Cloud Log Aggregation Warehouse (CLAW). It is based on a functional, module-based architecture, is hosted in multiple clouds, and it ingests, stores, and analyzes cloud security data and EINSTEIN sensor data from multiple agencies using commercial CSP services. It is geared toward enabling secure and efficient methods to process cloud data in a manner that offers CISA a similar level of situational awareness provided by current EINSTEIN on-premise deployments.

Figure 3 (below) shows a more detailed analysis of the shifting relationships for EINSTEIN implementation in the cloud. Roles that must be implemented or coordinated by more than one party are shown within the shared space of the overlapping ovals, with the participants identified. Traditional EINSTEIN was implemented almost entirely by CISA, with the agency only playing a role in provisioning a network tap for CISA use. This two-party interaction is shown below with roles labeled "Traditional NCPS (TIC)." For cloud telemetry, the agency, CISA, and CSPs each have a responsibility to enable functionality.

*Figure 3: NCPS Roles and Responsibilities*



## CISA Cloud Data Aggregation

CISA seeks to improve performance, to reduce costs, and to enhance threat discovery and incident responsiveness for agencies. CLAW is designed to support these goals by supporting agency adoption of cloud technologies. This section explains CLAW in more detail.

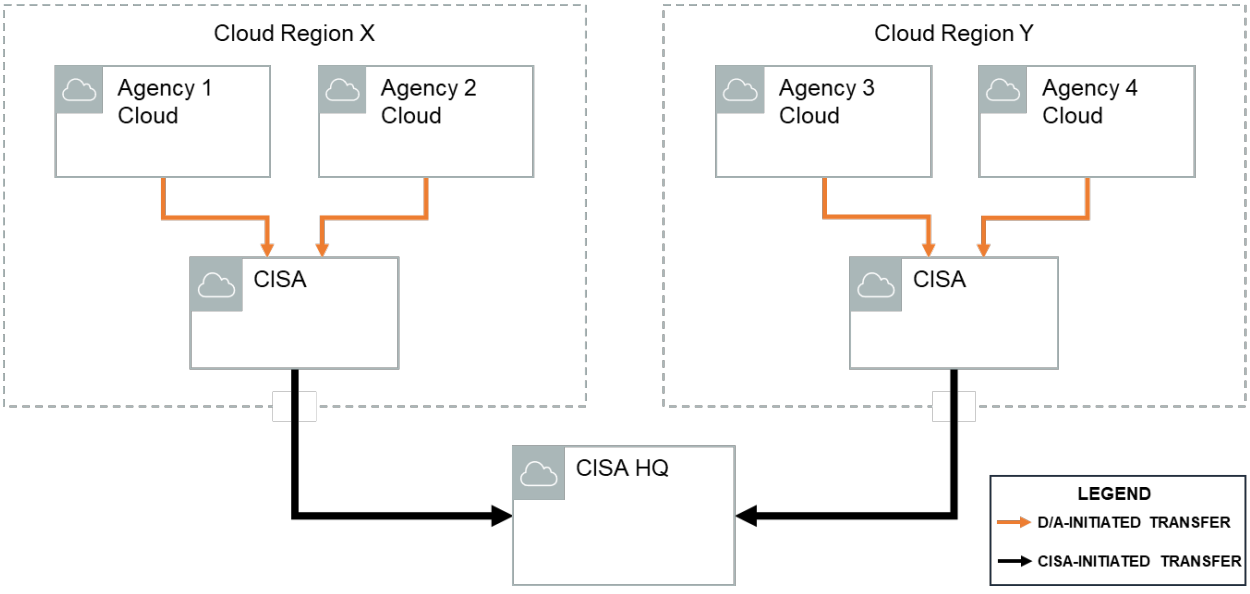
## Cloud Log Aggregation Warehouse Overview

CLAW is a CISA-deployed architecture for the collection and aggregation of security telemetry data from agencies using commercial CSP services. While agency security telemetry data currently is aggregated on-premise at CISA, CLAW is deployed in the cloud to aggregate agency security data that originate in the cloud. CLAW presents a functional, module-based architecture to ingest, store, and analyze security and sensor data from agencies. It is geared toward enabling secure and efficient methods to process cloud security data in a manner that offers CISA a similar level of situational awareness provided by current EINSTEIN on-premise deployments.

## CLAW Distribution

The CLAW architecture is being built to support security telemetry aggregation at multiple locations (optimized for performance, cost, and efficiency) utilizing centralized threat discovery with distributed analytics. Figure 4 depicts how agencies in different cloud regions can transfer their data to CLAW without requiring each to push its data to a single region.

*Figure 4: Responsibility for Transferring Security Data (Agency vs. CISA)*



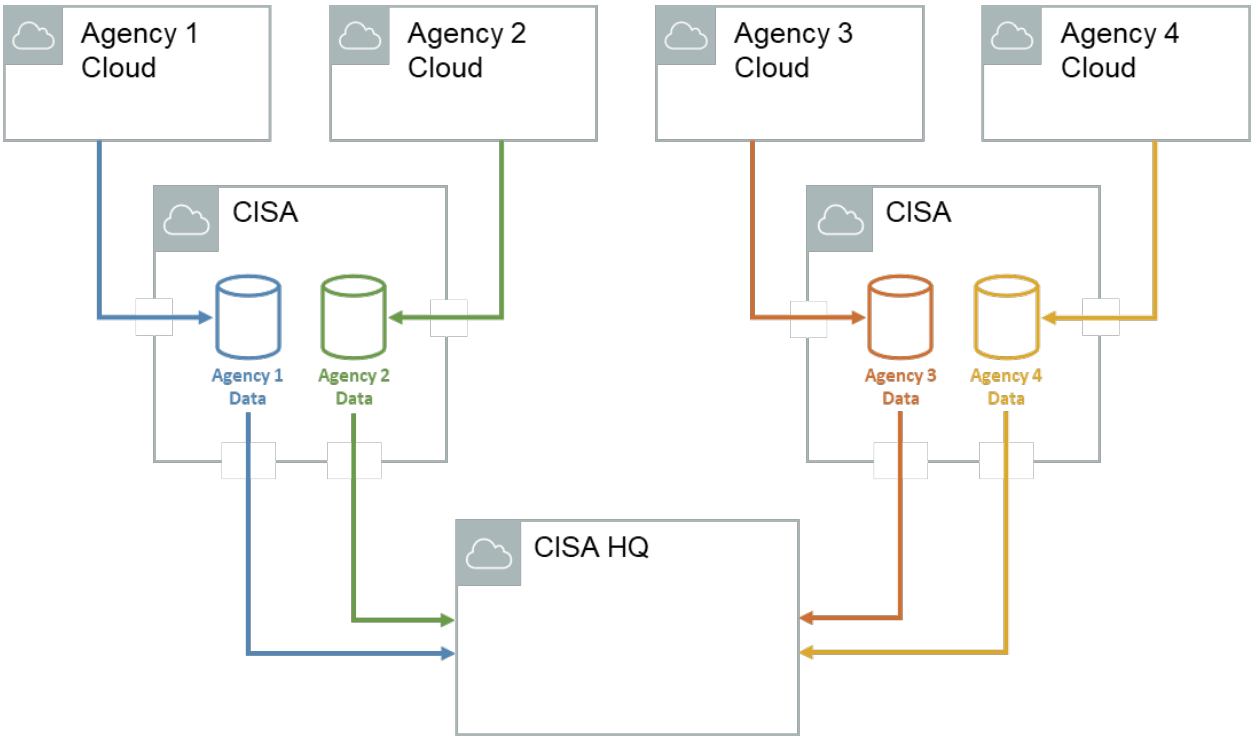

Agencies will be able to transfer their data to the closest CISA CLAW location based on their CSP and region, reducing data transfer costs, technical complexity, and transmission latency. The CLAW architecture supports collocating CLAW aggregation points with agency tenants on major CSPs. Any additional data aggregation or consolidation required will occur within CISA's purview.

**CISA Analysis of Agency Data**

Using CLAW, CISA provides the environment and tools to correlate and discover threats from application and network data that have been shared by agencies. Current analytics approaches involve signature-based (pattern recognition) and nonsignature-based (heuristic and statistical) analytics for identification of indicators of compromise and for identification of anomalous activities. Analysis will also bring in enrichment data to enhance the analysis results.

Figure 5 shows how cloud data from individual agency cloud tenancies is collected and analyzed at CISA cloud sites while preserving agency data isolation. Each agency's data are separated to prevent data comingling and corruption (using means such as independent data indexes and data stores). Analysis results obtained subsequently will be sent to CISA for processing and assimilation (i.e., for threat detection and correlation, and for synthesis of security indicators).

*Figure 5: Agency Log Ingestion (Autonomy Preserved with Log Isolation)*




Analysis will be coordinated from a central location with standardized tools. Those centralized tools will be able to interact with the sensor data distributed across CLAW locations. The data will be ingested and processed at a "local" CLAW location relevant to their CSP and region; in other words, the agency data will not be backhauled to a central repository. This will provide CISA cyber analysts with global situational awareness without requiring a corresponding centralized data store or requiring multiple copies of the same tools at each of the distributed data stores.

The data will be protected to ensure confidentiality and integrity using encryption for both data in transit and at rest that is compliant with Federal Information Processing Standard Publication 140-2.

In order to continue evolving NCPS, the program will continue to evaluate new intrusion detection and prevention methodologies utilizing native cloud services and cloud access security broker services.

**Modernizing the NCPS Core Infrastructure and Capabilities**

The NCPS Core Infrastructure is being transformed to use Federal Risk and Authorization Management Program-authorized commercial and government cloud services to the greatest extent possible, which will reduce greatly infrastructure investments at DHS data centers. Increasing utilization of commercial cloud capabilities for the NCPS core infrastructure and capabilities will improve the scalability, availability, and reliability of the infrastructure and capabilities that CISA needs. Overall, the NCPS Cloud Architecture is an overarching effort to integrate multiple cloud environments to include the adoption of SaaS applications. The NCPS cloud architecture is a hybrid cloud environment with common infrastructure management components identified to support monitoring, security and ease deployment of cloud environments. Modernizing the NCPS infrastructure includes several efforts that will evolve over time.

**NCPS Infrastructure Modernization**

The NCPS Cloud Business Exchange is a capability to support direct connections to the cloud and ISP environments to improve efficiency of acquiring security telemetry data from federal agencies and management of the NCPS Cloud Infrastructure. The NCPS program is modernizing the infrastructure to provide common views for provisioning and managing services across CSPs, ISPs, and on-premise locations while balancing the advantages of differentiated services. The NCPS Cloud Business Exchange will utilize Equinix, which provides direct-connect access to more than 300 CSPs and 1,700 ISPs through their networking fabric. Utilizing Equinix, the program will enhance network flexibility, will reduce the time to provision other cloud services and providers dramatically, reduces dependence on the ISPs, provides the ability to move data across low latency data circuits, and improves network performance by making each resource only one network hop away. Equinix allows tenants to deploy additional sites within hours from time of request of a new circuit for all sites already connected to Equinix.

Near-term efforts are focused on establishing the initial NCPS Infrastructure Modernization and Cloud Exchange environment. The environment will be expanded with additional sites being added to support failover and redundancy of capabilities. In the long term, NCPS will continue to enable direct connect access to CSPs and ISPs.

**NCPS Application Environment**

Efforts to modernize NCPS go beyond the infrastructure on which NCPS lives. Within the application environment, there are several efforts underway to modernize NCPS including:

- ***Cloud Analytics Environment*:** As we acquire more data, the NCPS infrastructure needs to evolve its data ingest, processing, and analytic environment to support discovery and analysis better across large data sets. NCPS is adopting new analytic tools to enable CISA cyber analysts to make sense of the data coming into the environment.
- ***Malware Next Generation*:** The Malware Analysis Environment is a platform used by CISA cyber analysts to receive, analyze, and correlate analysis of malware samples. The environment is being rearchitected in the cloud in order to improve the scalability, flexibility, modularity, resiliency, and interoperability of the environment. The Malware Next Generation environment will include improved automation to allow malware samples to be evaluated more quickly.
- ***Unified Workflow*:** Unified Workflow will provide a single platform for automating cyber operation workflows across independent business and mission support applications into a single infrastructure to improve the tracking, coordination, and reporting activities for CISA cyber analysts. This capability is utilizing a flexible SaaS platform with the ability to customize workflows and data models.

# IV. Conclusion

CISA needs a flexible environment that can anticipate and respond to evolving cyber threats. Efforts to modernize NCPS are focused on leveraging the rapid advancements of commercial and cloud-based technologies that will allow the program to respond quickly to the needs of CISA cyber analysts. Efforts surrounding CDM are focused on ensuring that the program remains operationally effective including identifying new capabilities and approaches for protecting government networks.

# Appendix - Abbreviations

| Abbreviation | Definition |
|---|---|
| CDM | Continuous Diagnostics and Mitigation |
| CFO Act | Chief Financial Officers Act of 1990 (P.L. 101–576) |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CLAW | Cloud Log Aggregation Warehouse |
| CSAB | Cloud Security Access Broker |
| CSP | Cloud Service Provider |
| DHS | U.S. Department of Homeland Security |
| DEFEND | Dynamic and Evolving Federal Enterprise Network Defense |
| E1 | EINSTEIN 1 |
| E2 | EINSTEIN 2 |
| E3A | EINSTEIN 3 Accelerated |
| FY | Fiscal Year |
| .govCAR | .gov Cyber Architecture Review |
| HVA | High-Value Asset |
| IOC | Indicator of Compromise |
| ISP | Internet Service Provider |
| IT | Information Technology |
| NCPS | National Cybersecurity Protection System |
| OMB | Office of Management and Budget |
| P.L. | Public Law |
| SaaS | Software as a Service |
| SOC | Security Operations Center |
| TIC | Trusted Internet Connection |