SECURE CLOUD BUSINESS APPLICATIONS (SCUBA)

Technical Reference Architecture

June 2023

Cybersecurity and Infrastructure Security Agency

Contents

1. INTRODUCTION

1.1 BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce cyber risks. CISA's roles include serving as the operational lead for federal civilian executive branch (FCEB) cybersecurity and providing cybersecurity tools, incident response services, and assessment capabilities. The FCEB IT enterprise requires continued, focused efforts to protect agencies against the sophisticated threats posed by both nation-state actors and other threat actors.

The Secure Cloud Business Applications (SCuBA) project provides architecture and guidance to address cybersecurity and visibility gaps in FCEB cloud business applications. These gaps impact each agency's ability to manage cyber risk for its IT enterprise and CISA's ability to manage cyber risk for the federal enterprise. The SCuBA architecture and guidance offer fundamental protections for cloud business applications and the necessary visibility to detect adversarial activity in the cloud.

Through the SCuBA project, CISA has the opportunity to:

a) expand the availability of its cloud security guidance to benefit both government and critical infrastructure partners;
b) expand utilization of available cloud security related data across existing and planned security programs;
c) improve program requirements and services;
d) leverage commercially available products and expertise from industry service providers; and
e) help secure cloud business application environments across the federal enterprise.

1.2 PURPOSE

The SCuBA Technical Reference Architecture (TRA) provides context, standard views, and terminology that incorporates and aligns all of SCuBA's efforts. The SCuBA TRA is product and vendor agnostic; consistent with federal cloud security guidance (*see* Section 4. Cloud Security Guidance *infra*); and based on the Cloud Security TRA published by CISA, the United States Digital Service, and the Federal Risk and Authorization Management Program (FedRAMP) [3]. This TRA provides threat-based guidance to inform product-specific security baselines and support agencies' secure adoption of cloud business applications—it does not supersede existing federal requirements.

A secure cloud business application (as defined in Section 3 *infra*) deployment requires a combination of application configurations, security services (provided natively with the application or by a third party), integration with existing enterprise systems, and robust operational practices. CISA engages with FCEB agencies to facilitate continuous acquisition of agency cloud logs and telemetry for CISA analysis and, when needed, to facilitate incident

response and threat-hunting activities. CISA will continue to work with agencies to address risks and maximize benefits associated with their use of cloud business applications.

CISA also consults with cloud vendors to identify opportunities to develop and improve solutions that provide enhanced security and support for cloud business applications used by FCEB agencies. Cloud vendors occupy a specific vantage point because they can identify trends and threat activities across sectors and service offerings. Cloud vendors also respond to threats that may be undetectable to their tenants, and they continuously update their offerings to mitigate vulnerabilities and adversarial campaigns.

For the SCuBA TRA to function consistent with federal requirements, such as the Office of Management and Budget (OMB) M-21-31 [4], agencies must work with CISA to implement comprehensive logging and information-sharing capabilities. This coordination includes agencies sharing telemetry and logs from their cloud business applications with CISA. CISA needs this information to have the visibility and capacity to respond to evolving cloud threats and perform effective monitoring, threat hunting, and incident response activities. In turn, CISA shares threat information that allows agencies to collect, process, and analyze telemetry to fulfill their own internal security requirements, enhance their visibility, and meet mission needs.

As agencies secure and monitor their cloud business applications, they need to align with the Zero Trust (ZT) principles and requirements of OMB M-22-09 [5]. This TRA supports agencies' meeting of several OMB M-22-09's requirements for applications, workloads, and data.

1.3 SCOPE

The SCuBA TRA's scope encompasses cloud business applications, delivered through a Software as a Service (SaaS) model to users and security services agencies to use to protect and monitor their cloud-based applications. Figure 1 shows that an agency is responsible for securely configuring their cloud business applications and collecting the associated logs and telemetry to meet their security needs. The cloud service providers (CSPs) are responsible for securing the underlying infrastructure, which is out of the scope of the SCuBA TRA.

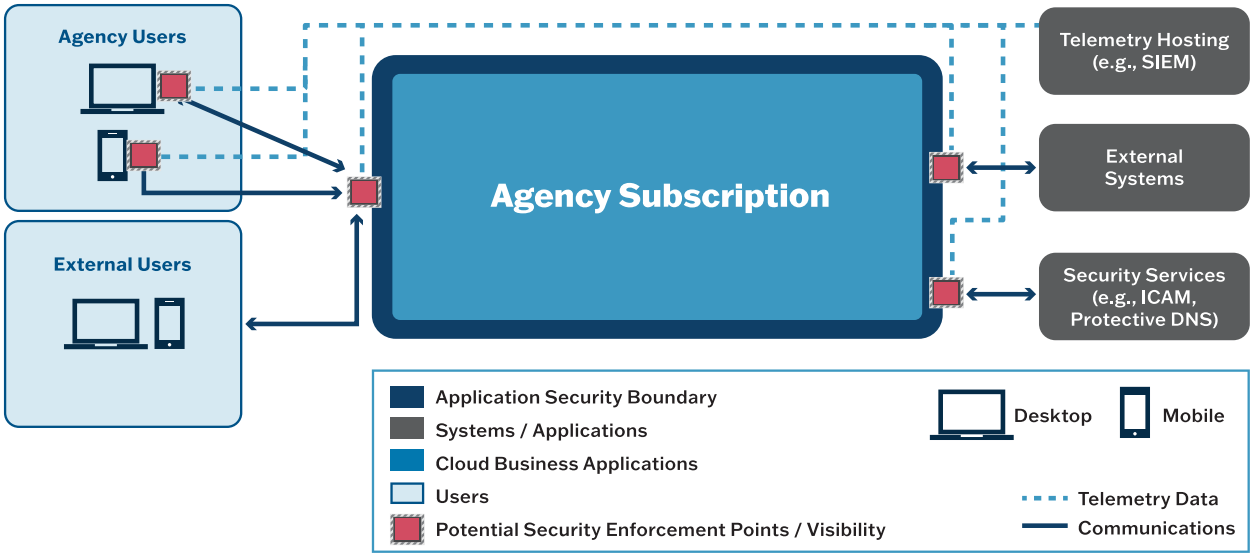

Figure 1. SCuBA system view

Agency Users

The SCuBA TRA's scope includes connections from campus and internet sources. Agencies' ZT strategies may change how their users access their cloud business applications. Users can access their cloud applications through agency endpoints via desktop, virtual, or mobile. Consequently, it is important to note what is out of SCuBA TRA's scope:

1. The management and security of the endpoints.
2. Bring Your Own Device.
3. Dedicated telephony devices, such as desktop phones using Voice over Internet Protocol or Time Division Multiplex signaling.

External Users

External users include both trusted business partners and the public who use the collaboration tools for voice and video and document/content sharing.

Agency Subscribed Cloud Business Applications

The initial set of cloud business capabilities are based on FCEB agencies' implementations. These capabilities—which currently include productivity, messaging, content management, collaboration, and voice—may expand in the future as other cloud business applications evolve. See Section 3 for more details regarding the cloud business capabilities' scope.

2. DEVELOPMENT

The SCuBA TRA is based on input across CISA programs and services, analysis and identification of cloud security guidance, applicable supporting documents (*see* Section 4 *infra*), identification of cybersecurity threats (*see* Section 5 *infra*), and necessary security capabilities to harden cloud business applications (Section 6 *infra*).

If necessary, CISA will periodically update the SCuBA TRA to ensure it is relevant and current. Updates will be based on lessons learned from other cloud efforts—including SCuBA—such as product-specific testing, configuration guidance, capabilities, and instance architectures. Updates will come from input from FCEB agencies, collaborations with CSPs and commercial organizations with mature cloud implementations and cloud threat assessments, and testing and input from cloud application and infrastructure security subject matter experts (SMEs). Figure 2 shows the SCuBA TRA iterative approach.

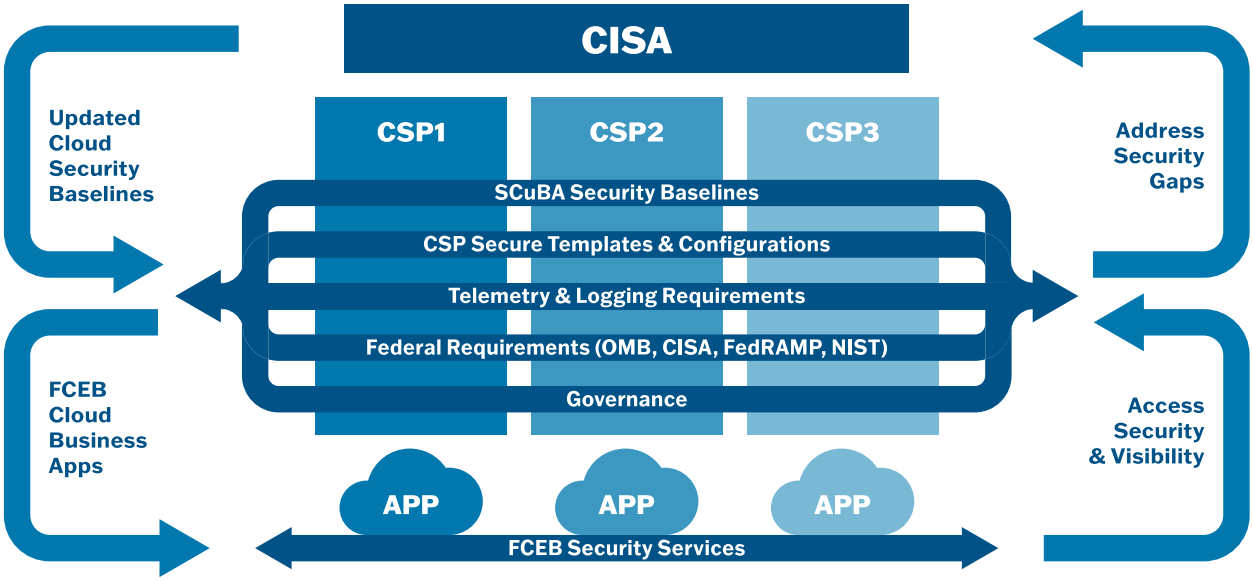

Figure 2. SCuBA TRA iterative approach

The SCuBA TRA supports CISA's objective to keep pace with evolving policies, requirements, and technical capabilities to inform solution architectures, address security gaps, and cover visibility needs. The SCuBA TRA accomplishes this objective through the following iterative approaches:

- **Building on Existing Knowledge:** CISA will build on the current knowledge of CSP and SaaS offerings to provide guidance based on understanding threats and related efforts. CISA will collaborate with the CSPs to improve SaaS offerings and how these provisions interface with security services.
- **CISA Cloud Security and SCuBA Baselines:** CISA will first gather and assess feedback and lessons learned from implementation within its own divisions before deploying baselines that respond to increasingly complex mission needs. Applying SCuBA security solutions to a wide range of agencies will require building on existing technologies and testing new capabilities.
- **Enabling a Feedback Loop:** As agencies deploy cloud solutions to meet mission needs and SaaS offerings change to reflect market demands, threats evolve to leverage new tactics, techniques, and procedures (TTPs). As a result, a feedback loop

will help continue refining engineering solutions and improving SaaS offerings' configuration guidance.

3. DEFINITION OF CLOUD BUSINESS APPLICATIONS

The business capabilities shown in Figure 3 define the initial version of the SCuBA TRA, cloud business capabilities.

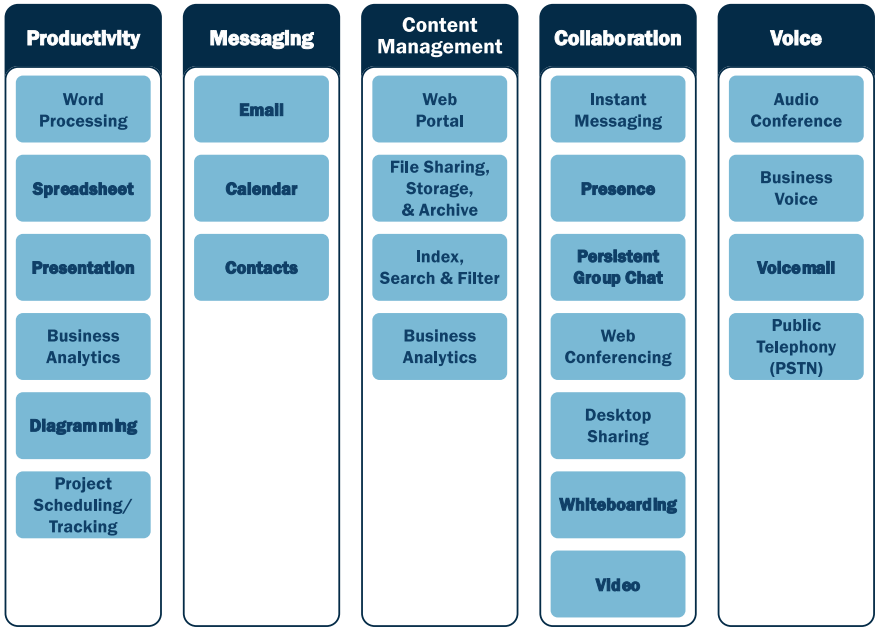

Figure 3. Cloud business capabilities

Figure 3 groups the capabilities into categories using vendor-agnostic terms (productivity, messaging, etc.) based on their functions. The examples under each category are not exhaustive but are representative of the scope's functions. Each category may have similar threats and security controls. Agencies can assess the threats and security controls necessary to protect their enterprise and provide CISA with the required visibility. The categories are:

- **Productivity:** Capabilities that allow users to perform business analytics and produce documents, graphs, spreadsheets, presentations, diagrams, project schedules, and trackers. These capabilities produce human readable objects that Messaging or Content Management capabilities can share.
- **Messaging:** Capabilities focused on email, using the calendar, and managing contacts.
- **Content Management**: Capabilities for website hosting, file storage and sharing, searching, and workflows.
- **Collaboration**: Capabilities that allow for real-time text, video, and desktop sharing and that use productivity capabilities as an integrated function of the Collaboration capabilities.

- **Voice:** Capabilities focused on telephone-based functions, either initiated from a phone (mobile or wired) or connected to the Public Switched Telephone Network.

4. CLOUD SECURITY GUIDANCE

The following subsections provide details regarding the cloud security guidance documents that informed SCuBA TRA's development.

4.1 CISA CLOUD SECURITY GUIDANCE

CISA Cloud Security Technical Reference Architecture

The Cloud Security TRA—coauthored by CISA, the United States Digital Services, and the Federal Risk and Authorization Management Program—is a guide for agencies to use for adopting cloud technology for cloud deployment, adaptable solutions, secure architecture, agile development, and ZT principles [3]. This guide discusses key topics and concepts aligned with shared services, cloud migration, and cloud security posture management. Various sections of the SCuBA TRA correspond to the Cloud Security TRA including identity, credential, and access management (ICAM), logging, monitoring, and shared services.

CISA NCPS Cloud Interface Reference Architecture Volumes 1 and 2

The National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture (RA) is a two-volume collection that explains how agencies create reporting patterns to describe their process for providing cloud-generated security information to CISA's Cloud Log Aggregation Warehouse. Volume 1 defines general reporting patterns [6]. Volume 2 is a catalog of reporting patterns typical of how agencies send telemetry from a single CSP or from multiple providers [7]. Together, these two resources describe multiple options for sharing cloud telemetry with CISA, but do not define specific requirements for what cloud telemetry is shared. CISA uses a framework to define telemetry requirements, called the extensible Visibility Reference Framework (eVRF) described later in Section 4.

CISA Trusted Internet Connections 3.0 Core Guidance and Use Cases

The Trusted Internet Connection (TIC) 3.0 core guidance is comprised from the Program Guidebook, the RA, the Security Capabilities Catalog, the Use Case Handbook, and the Overlay Handbook [8]. Agencies can use these guidance documents collectively to develop and deploy modern architectures:

- The Program Guidebook outlines the TIC Program and explains its history.
- The RA defines the key technical concepts that define TIC 3.0 architectures.
- The Security Capabilities Catalog is a library of security capabilities used in TIC 3.0 use cases.
- The Use Case Handbook describes how agencies can create and use TIC use cases.
- The Overlay Handbook defines how vendors can map their products and services to the TIC security capabilities.

Additionally, TIC 3.0 use cases contain guidance on the secure implementation and/or configuration of specific platforms, services, and environments. In accordance with OMB M-19-26, CISA has published the following use cases: (1) Traditional TIC Use Case, (2) Branch Office Use Case, (3) Remote User Use Case, and (4) Cloud Use Case (Draft). These publications contain specific guidance for agency infrastructure as a service (IaaS), platform as a service (PaaS), SaaS, and environment as a service (EaaS) deployments. Each TIC use case contains conceptual architecture, risk and deployment considerations, one or more security pattern options, and security capability implementation guidance for a common agency computing scenario. Agencies can combine use cases to modernize their enterprise.

Continuous Diagnostics and Mitigation

The SCuBA TRA will continue to draw insight and guidance from the CISA Continuous Diagnostics and Mitigation (CDM) Program to provide a dynamic approach to fortifying government network and system cybersecurity [9]. The CDM Program will continue to deliver cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture. Additionally, the CDM Program continues developing guidance for agencies focused on the integration of cloud platforms into CDM dashboards.

CISA Zero Trust Maturity Model

CISA's Zero Trust Maturity Model (ZTMM) goal is to assist agencies in developing their ZT strategies and implementation plans. The ZTMM presents a gradient of implementation across five distinct pillars, where advancements in maturity can be made over time. The model also presents ways in which various CISA cybersecurity programs support ZT solutions across agencies. The SCuBA TRA aligns with ZTMM's Application Workload pillar for agencies' cloud business applications outcomes.

Extensible Visibility Reference Framework Guidebook

The extensible Visibility Reference Framework's (eVRF) purpose is to define the concepts, requirements, and mechanisms for CISA, FCEB agencies, and other partners to identify, collect, and evaluate cyber visibility to mitigate threats [10]. The eVRF Guidebook is an instruction manual for eVRF—defining and describing key concepts, roles and responsibilities and workflows [11], including CISA telemetry requirements, and identifying the demand for visibility as a specific cybersecurity characteristic, with a structure and workflow that define visibility for different portions of a digital environment. The eVRF workbooks define specific visibility surfaces that agencies can implement using an Excel spreadsheet or a software application, The eVRF workbooks will continue to evolve over time.

4.2 FEDERAL CLOUD SECURITY GUIDANCE

Federal Risk and Authorization Management Program

FedRAMP provides a standardized approach to security authorizations for cloud service offerings [12]. This program accredits cloud service offerings for the federal government,

adopts innovative cloud services to meet agency mission needs, and oversees periodic security assessments by third-party assessment organizations. The cloud business application will follow the FedRAMP authorization process to properly authorize the cloud service offering. Compliance with FedRAMP is mandatory for all executive agency cloud deployments and service models at the low-, moderate-, and high-risk impact levels [13].

OMB Memorandum: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

The OMB Zero Trust Architecture (ZTA) strategy memorandum M-22-09 establishes specific cybersecurity standards and objectives for agencies to fulfill as part of their adoption of ZT architectures [5]. The SCuBA TRA aligns with these objectives and standards. Agencies should consider the actions specified in the memo and their own ZT strategies and planning when designing and implementing security for their cloud business applications to ensure they meet ZT goals.

OMB Memorandum: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

The OMB memorandum M-21-31 sets out logging, log retention, and log management requirements for agencies [4]. Although its requirements are broader than cloud environments, they do apply to cloud environments. Consequently, agencies need to ensure they continue to fulfill these requirements in deploying and maintaining their cloud business applications.

Federal ICAM Architecture Introduction

The Federal Identity, Credential and Access Management (FICAM) Architecture Introduction describes the basics of ICAM, the FICAM architecture, and how to use the information to facilitate enterprise ICAM practices at an agency [14]. See Section 6.1 for additional information.

5. THREATS TO CLOUD BUSINESS APPLICATIONS

As the threat landscape is constantly evolving, an authoritative source for tracking, documenting, and mitigating threats is imperative. To inform an architecture to secure cloud business applications, use multiple sources for characterizing threats. Threat identification sources for cloud applications are either open-source or closed source (proprietary/classified). The MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework will be the primary open-source taxonomy for characterizing threat sources and TTPs for SCuBA.

The MITRE ATT&CK matrix for SaaS and relevant vendor-specific matrices will outline security threats. The MITRE ATT&CK framework is a knowledge base resource and a taxonomy for cyber adversary behavior. The framework outlines various phases of a cyberattack lifecycle and targets malicious cyber actors are known to exploit. ATT&CK includes only adversarial

tactics and techniques based on real-world observations as of the date of the posted matrix, reducing its ability to characterize novel or emerging adversarial activities. The eVRF accounts for these emerging threats by characterizing the visibility available for cloud business applications, regardless of the specific attacker actions catalog status in ATT&CK. eVRF further permits mapping the observations to the ATT&CK techniques applicable to the business applications domain. In this way, eVRF visibility surface definitions and coverage maps can identify visibility that should be available and characterize the available visibility within a given system, respectively. See Section 6.7 for additional details.

6. SECURING CLOUD BUSINESS APPLICATIONS

This section describes the essential components of security services and capabilities to secure and harden cloud business applications. These security services and capabilities prevent and mitigate vulnerabilities and threats from affecting the cloud business applications during implementation, configuration, and administration. In addition, once in place, these security services and capabilities harden the system to improve the cloud business applications' security and the platform that hosts the applications.

The previously identified business capabilities, threats to those capabilities, and related federal and CISA efforts determine the set of configurations and security services. Agency-specific implementations of these services should follow their specific risk profiles and tolerances. These security configurations, when monitored in real time or near-real time, serve as a proactive security approach to identify potential cybersecurity threats and help safeguard, monitor, and maintain the environment.

Figure 4 illustrates the SCuBA security and visibility points. Each point maps to one or more relevant sections of the SCuBA TRA, as shown in Table 1. Additionally, from a ZT perspective, while the security of these applications intersects with each of the ZT Maturity Model pillars, the application security boundary most closely aligns with the application workload pillar.

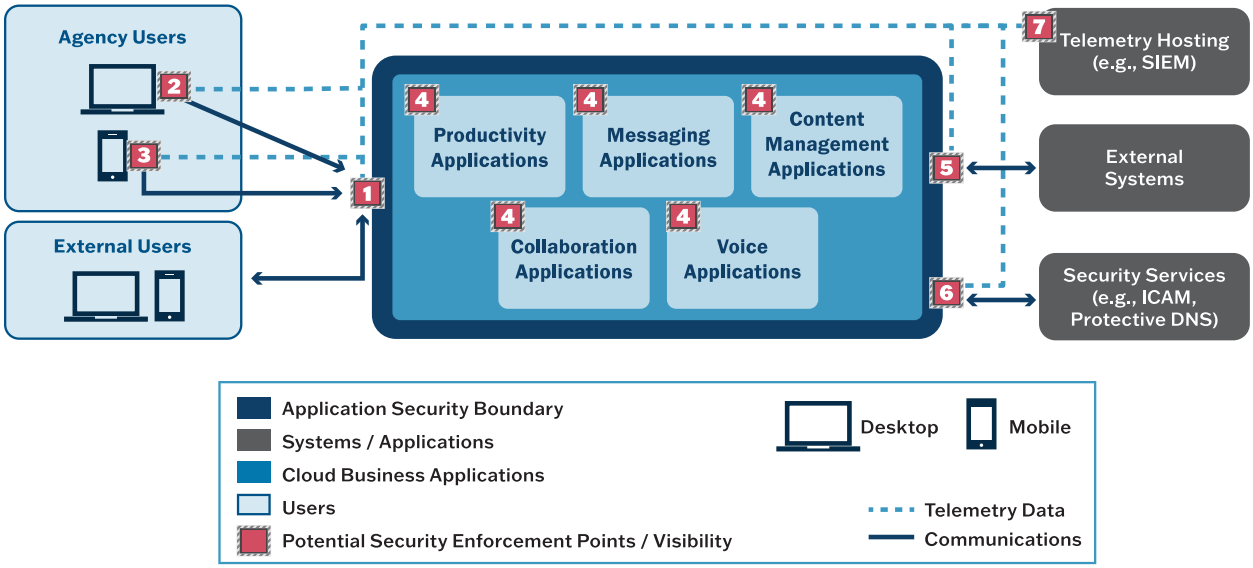

Figure 4. SCuBA security and visibility view

Table 1 maps the numbered security and visibility points to the relevant subsections that provide detail.

Table 1. Security and Visibility Mapping to Sections

Security Enforcement Point/Visibility	Relevant Sections
1	Section 6.1 Identity, Credential and Access Management Section 6.2 Secure Cloud Access from Any Location Section 6.4 Protective Domain Name System (pDNS) Section 6.6.1 Data Sharing and Exfiltration Protection
2	Section 6.1 Identity, Credential and Access Management Section 6.5.1 Desktop Endpoint Security
3	Section 6.1 Identity, Credential and Access Management Section 6.5.2 Mobile Endpoint Security
4	Section 6.6 Application Security Configuration
5	Section 6.3 External Email Protections Section 6.6.1 Data Sharing and Exfiltration Protection
6	Section 6.1 Identity, Credential and Access Management Section 6.4 Protective Domain Name System
7	Section 6.7 Cyber Visibility and the eVRF Analytical Framework Section 6.8 Telemetry Generation and Processing

Security Enforcement Point/Visibility	Relevant Sections
All	Section 6.7 Cyber Visibility and the eVRF Analytical Framework Section 6.8 Telemetry Generation and Processing Section 6.9 Shared Responsibility Model

6.1 IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

Identity, Credential, and Access Management (ICAM) is a core tenet of ZT, and it facilitates cybersecurity risk management decisions. "ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, and for the right reason, in support of federal business objectives [14]." The Government Services Administration (GSA) provides guidance on establishing an ICAM program through the implementation of FICAM architecture and the National Institute of Standards and Technology's (NIST) Special Publication 800-63-3, *Digital Identity Guidelines*. The FICAM architecture provides the overarching architecture for establishing requirements and guidelines for an ICAM program. NIST's Special Publication 800-63-3 provides guidance to determine various levels of identity proofing, registration, authenticators, authentication protocols, and federation for agencies implementing digital identity services [15].

Typically, agencies have a pre-existing ICAM program such as the one shown in Figure 5. This infrastructure provides central management of identities, issues logical credentials (typically personal identity verification (PIV) cards or derived PIV credentials), and, in some advanced cases, provides central management of roles or entitlements.

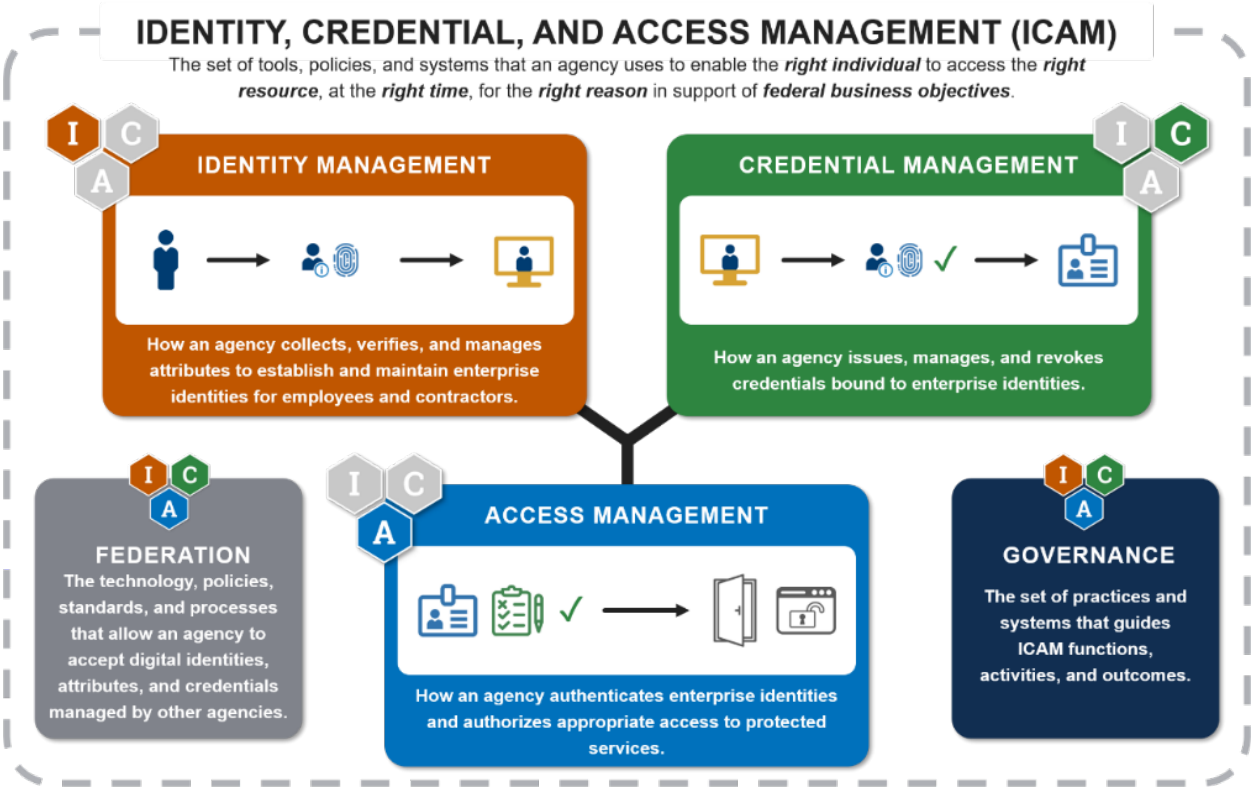

Figure 5. ICAM practice areas and supporting elements [14]

A common business application deployment is to federate the pre-existing ICAM infrastructure (e.g., through Microsoft Active Directory Federated Services) with the business applications. Various configurations are possible, but the details are out of scope of this document. However, because such a deployment reuses pre-existing infrastructure, certain cybersecurity compromises on-premises infrastructure, which could also pose risks to the cloud. The FICAM architecture provides guidance to the federal government to design, plan, and execute common ICAM processes [14]. FICAM recommends only the federation of end-user accounts. The FICAM recommendation is based on the OMB ZTA strategy M-22-09, which states that "Agencies must require their users to use a phishing-resistant method to access agency-hosted accounts[5]."

An alternative architecture gaining popularity for agencies leverages a cloud-based identity as a service (IDaaS) provider for authentication directly in the cloud (e.g., using a PIV-based credential). Such an architecture adopts a shared responsibility model in which the IDaaS provider assumes responsibility for security of key platform components (e.g., cryptographic material required for federation protocols) while the agency remains responsible for secure configuration. In this model, the agency, the vendor, and CISA share some responsibilities, such as monitoring for threats. CISA recommends that agencies explore, in detail, the tradeoffs between these two models as relevant to their existing environment and mission goals.

ICAM is critical to securing a cloud application. Many parts of ICAM require enterprise-wide management (identity lifecycle, issuance of root credentials and privilege role assignment, etc.). However, some parts of access management are configured specifically within the cloud business applications. This is especially true for managing end-user access. One important aspect is strong administrative controls and the lowest level privilege. Cloud business application least privilege policies enable limiting access only to authorized and up-to-date devices. Such policies tie together the secure cloud access (SCA) and endpoint protection technologies. These policies "close the loop" by ensuring that only devices that follow the agency's desired security posture can access agency data. CISA is developing secure configuration baselines specific to cloud-native identity and access management services for Microsoft 365 (M365) [10] and Google Workspace (GWS) to support these identity- and access-focused considerations. CISA may develop additional product baselines as FCEB agencies use other cloud business applications.

6.2 SECURE CLOUD ACCESS FROM ANY LOCATION

With the growth of mobile, telework, and cloud applications, traditional approaches to secure cloud access no longer meet FCEB needs. The TIC program recognizes this change and articulates a new model for securing access to cloud applications. The SCuBA TRA uses the TIC 3.0 guidance as the foundation for securing user access to business applications using SCA products and services. SCA solutions should be part of agencies' cloud business application deployment. In the broader cloud market, vendors use terms such as ZT Network Access, cloud access security broker (CASB), secure email gateway (SEG), secure access service edge (SASE), and other terms to refer to products and services that target different SCA aspects. The broader market is rapidly evolving as these discrete solutions converge.

SCA solutions give users the ability to securely access the agency's business applications that reside on a CSP. These business application users may be on the enterprise network, in a branch office, on a remote device, or on a mobile device. The SCA solution, along with the security services embedded in the destination CSP and the source workstation or device (e.g., endpoint detection and response (EDR)) follow the TIC guidance. Different use cases and security patterns may require other technical solutions. Some SCA solutions may enhance visibility and risk determination using information received from agents hosted by either managed or unmanaged endpoints (e.g., trusted business partners). SCA security functions may be the same as, or complement, the source workstation or device and CSP security functions. For example, the CSP might provide SCA functions, the source workstation or device, a third-party vendor, or all these components. See Figure 6 for an illustrative overview of an SCA concept.

The SCuBA TRA only introduces the SCA topic. TIC 3.0 guidance documents provide additional information for design alternatives for different SCA use cases.

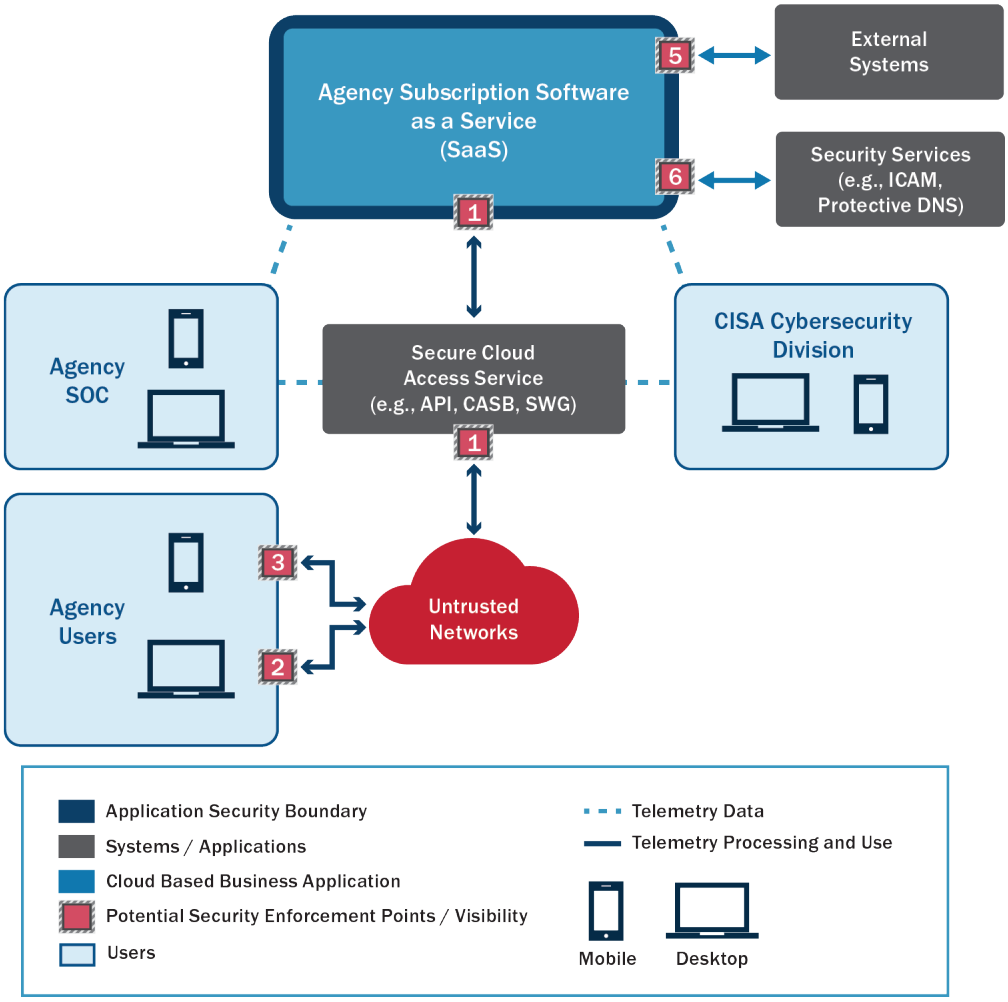

Figure 6. SCA concept

6.3 EXTERNAL EMAIL PROTECTIONS

Email is often used as an entry point to agency environments, as shown in Figure 7. Adversaries use it to deliver both phishing links and malware, as seen in recent high-visibility incidents. Email-related risks are typically addressed with a combination of native security capabilities built into the CSP's products and independent third-party offerings. Typically, email security solutions (whether provided as a native security capability in a CSP offering or as a separate product) include the following:

- **Filtering and Tagging**: Email filtering of all messages (e.g., ingress, egress, internal) for detecting malware, identifying spam, and tagging for agencies. This includes using both government (i.e., CISA, agency) and commercial indicators and attributes (behavioral and reputational) for malware detection, and spam identification and tagging for agencies. Email filtering and tagging includes using both government (i.e., CISA, agency) and commercial indicators and attributes (behavioral and reputational).

- **Log Visibility**: CISA and agency security operations personnel should have visibility into email attributes.
- **Authentication and Integrity**: Modern techniques for ensuring that sending and receiving email servers are mutually authenticated and messages are not manipulated in transit. This is accomplished using domain-based message authentication; reporting; and conformance, sender policy framework, and domain keys identified mail.
- **Additional Features**: Other key features in robust email security protections include automated indicator provisioning, threat intelligence, advanced analytics, reporting, cyber hunt support and incident response, sandboxing, detonation, and the ability to incorporate third-party security services.

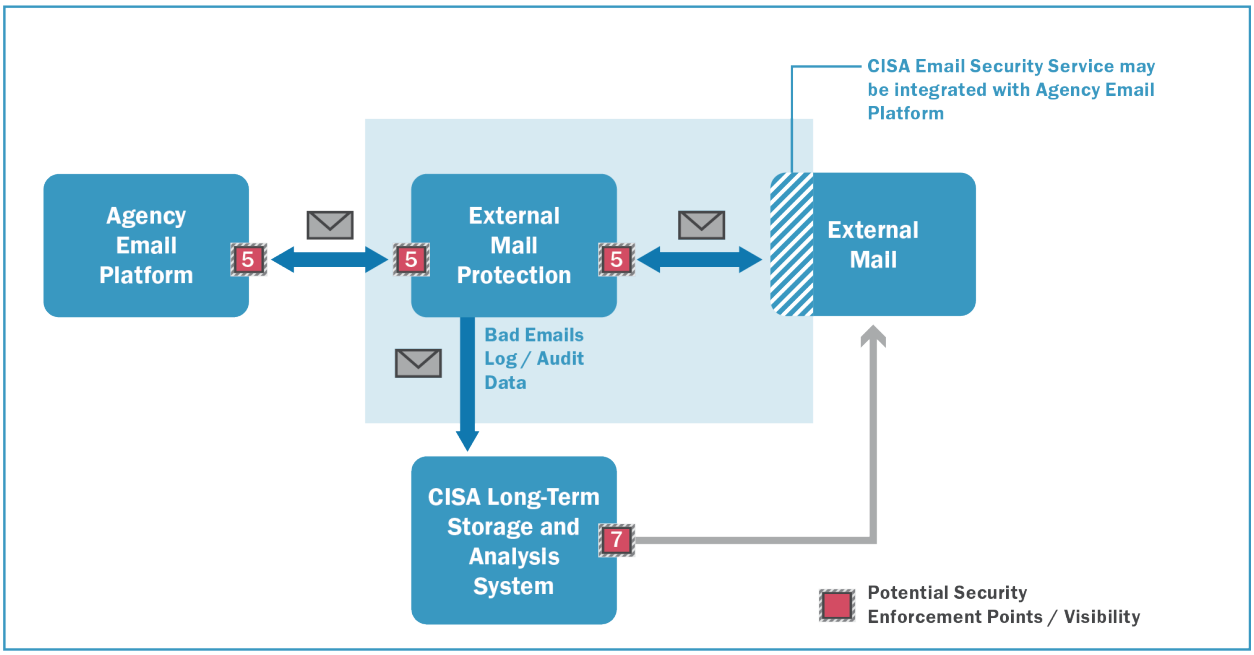

Figure 7. External email flow

CISA is also developing secure configuration baselines (see Section 6.6) for email security. Identity-related configuration requirements and baselines in development also support email security. Agencies should integrate external email protections and implement secure configuration baselines for critical cloud services that affect email security, such as Exchange Online, Azure Active Directory, Google Cloud Identity, or other third-party vendors. CISA offers new domain name system (DNS) capabilities and is developing a modern protective email services (PES) that will improve email security and eventually replace E3A services.

6.4 PROTECTIVE DOMAIN NAME SYSTEM

In addition to SCA solutions that apply policy to and collect telemetry from network flows between endpoints and cloud applications, DNS lookup provides a widely used insertion

point in internet infrastructure to implement cybersecurity policy and visibility. The CISA Protective DNS solution includes these key capabilities:

- Internet protocol (IP) v4 and v6 source address verification.
- Query filtration by IP, domain, subdomain, or record type.
- Auto-blockage of newly created domains, "look-alike" homoglyphs, nonstandard query structures, and known risky domains.
- Self-monitoring heuristics to gauge percentage of correctly permitted (benign) queries, correctly blocked (malign) queries, and anomalous false positives.
- Direct bypass, for use cases in which crucial DNS queries must go through.
- Location blocking.
- DNS over transport layer security (DoT) and DNS over hypertext transport protocol secure (DoH).
- Telemetry collection for both the agency and CISA (i.e., to discover outbound Command and Control traffic).

CISA's new DNS capabilities will modernize and eventually replace the current E3A domain sinkholing functionality. Agencies should deploy the CISA Protective DNS security solution or equivalent protective DNS capabilities, including customizable DNS query filtration, such as "allow," "deny" (block), "overwrite" (rewrite) response, or "sinkhole" (suppression) based on domain parameters, encrypted DNS support, DoT support, DNS security extensions support, and compatibility with current Internet Engineering Task Force (IETF) DNS protocol extensions.

6.5 ENDPOINT SECURITY SERVICES

Managing all endpoints (including mobile, server, virtual machine, and desktop) is critical to securing cloud business applications and to support a ZT approach. Although mobile security is not within the ScuBA project's scope, expect that agencies need to deploy and configure their cloud business applications to enable secure access from their mobile and desktop devices.

6.5.1 Desktop Endpoint Security

SCuBA relies on endpoint security technologies for both policy and visibility. Configure the cloud business application access policies to limit access to agency data based on host posture assessment (see Section 6.6). Specifically, the policies should enforce that all sensitive data requests come from agency-managed devices that comply with agency endpoint security policies, such as operating system version and patch level (or devices explicitly authorized by risk-based policy decisions supporting mission needs). These endpoints include desktops, laptops, and virtual machines. Use EDR products to collect the signals necessary to make these policy decisions and provide critical visibility into the endpoints that enable cybersecurity response.

Agencies should leverage the CDM Program to obtain and deploy EDR technologies in their environment. Additionally, configure the cloud business application to leverage signals from the EDR products to govern access to private agency data. See OMB Memo 22-01 for more information on the applicability of EDR [16].

Limited opportunities exist for agency policy enforcement or evaluation for endpoints the agency does not manage, such as those of guests, collaborators, partners, customers, or even agency users' personal devices. The breadth of access to agency data reflects this limited insight by reducing or even prohibiting access to sensitive information.

6.5.2 Mobile Endpoint Security

Configure similar access policies for agency-managed mobile endpoints. To protect and manage mobile devices and applications, the CDM Program helps agencies deploy enterprise mobility management (EMM) capabilities [17]. EMM solutions enable agencies to manage device configuration and device compliance, monitor and track devices, manage allowed mobile apps, detect and address malicious mobile apps via mobile threat defense and mobile application vetting, discover and respond to network-based attacks and vulnerable configurations, and support the issuance and life cycle management of credentials provisioned on mobile devices. Configure agencies' cloud business applications to leverage signals from EMM solutions in access decisions.

CISA also published Capacity Enhancement Guides to help enterprises and consumers improve mobile device cybersecurity [18]. To support agencies as they develop their ZT plans and roadmaps, CISA developed a whitepaper titled "Applying Zero Trust Principles to Enterprise Mobility [19]." The paper describes mobile security technologies, explains how mobile security technologies support ZT principles, and identifies areas requiring additional work.

6.6 APPLICATION SECURITY CONFIGURATION

As the federal government continues to move critical services to the cloud, it is imperative to ensure consistent, effective, modern, and manageable security configurations to protect all information assets in and connections to cloud services. This initiative's objective is to move federal cybersecurity forward by helping agencies keep pace with sophisticated and determined cyber threats. At the time of this writing, the SCuBA project is developing and testing minimum viable security baselines for easy and quick adoption across the federal civilian landscape. A "Security Baseline" defines a set of basic security objectives that must be met by any given service or system. (See Figure 2 for a visual representation of where these artifacts sit within the iterative approach to the SCuBA TRA development.)

Agencies using M365 and GWS can adopt these recommended cybersecurity configurations, which is a key benefit. Maintaining and updating this guidance is essential to ensuring an acceptable and consistent security posture. CISA leads these efforts with input and support from interested federal agencies. The baselines are also developed with an eye towards

automation rather than manual repetitive tasks where possible, improving consistency in application, and reducing time to deployment.

The baselines cover the full scope of the security architecture for SCuBA, including ICAM, collaboration, cloud access security broker capabilities, threat intelligence, detection, mitigation, cloud storage, cloud-native email service security, and cloud-native business applications. Baselines selection may increase as CISA continues maturing SCuBA.

6.6.1 Data Sharing and Exfiltration Protection

Another key SCuBA security concern is data exfiltration risk. Agencies must balance the need to collaborate with other stakeholders outside the agency (and thus share content, calendars, etc.) with the need to protect agency data. At a minimum, agencies should use cloud business applications' built-in rules systems to detect cross-tenant data sharing. Used correctly, these rules can help discover exfiltration of important agency data. In some cases, agencies may also choose to block cross-tenant sharing of certain types of data (e.g., share busy/free status but not documents), depending on mission requirements.

6.7 CYBER VISIBILITY AND THE eVRF ANALYTICAL FRAMEWORK

Agencies will need to collect and apply cyber visibility, both operational and technical (e.g., insights into assets, users, systems, data, events, an logs), to detect indicators of attack (IOA) and indicators of compromise (IOC) associated with the use of cloud business applications. Activities include applying key eVRF concepts. The *eVRF Guidebook* defines the concepts, requirements, and mechanisms for CISA, FCEB agencies, and other partners to collect and apply cyber visibility to mitigate threats. In the context of SCuBA, an applicable eVRF concept is that of the visibility surface, defined as "a digital environment for which cyber-observable data exists or should exist [10]." Essential parts of this digital environment include application logs, endpoint access logs, proxy logs, service logs, reports, and alerts generated with the monitoring, auditing, and alerting services that provide evidence of malicious and benign activity. Section 6.1 identifies potential sources for such telemetry. Threat-detection services the cloud business application providers or third-parties offer (see Section 6.8.5 Threat Prevention or Detection and Mitigation) should communicate detected anomalies, prevent threats, and apply mitigations. Analysts from agencies, CISA, and vendors each have a specific role and associated visibility demands for telemetry from sources stored in the Telemetry Hosting solution. When deploying and configuring services to ensure coverage, accommodate the visibility demands. The eVRF workflow can assist in characterizing visibility completeness.

The *eVRF Guidebook* identifies three workflow phases for accomplishing cyber visibility: (1) define visibility surface, (2) produce visibility coverage maps, and (3) generate coverage comparisons for analysis and insights [11]. Figure 8 describes these process phases and includes a detailed description for each. The referenced document [10] provides the execution steps.

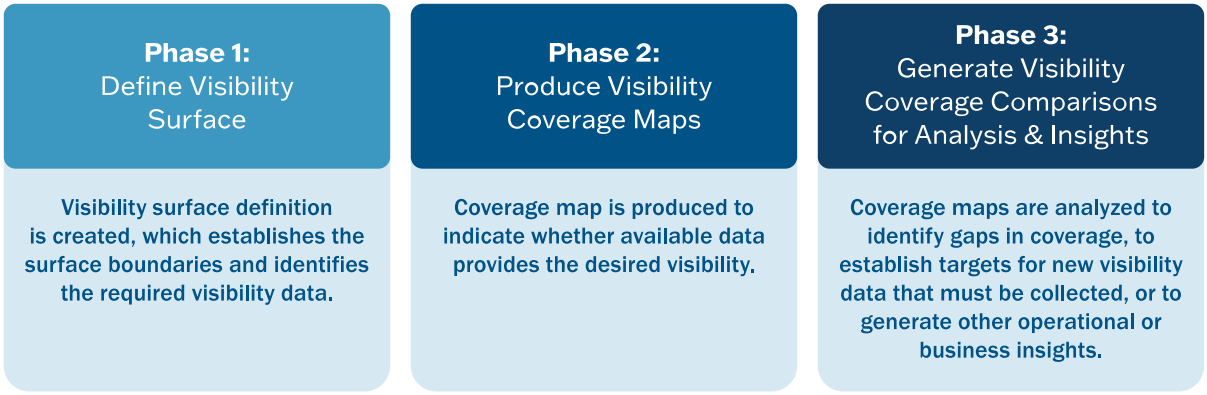

Figure 8. eVRF workflow

The *eVRF Guidebook* identifies roles and responsibilities for CISA, organizations (agencies), and vendors/service providers [11]. In summary, CISA is responsible for developing an eVRF visibility surface definition and requirements coverage map in an eVRF workbook. The eVRF workbook guides agencies in their internal policies and aligns with CISA's cyber visibility requirements. Vendors/service providers can use the workbook to reduce or eliminate visibility gaps in their offerings and comply with eVRF.

Use a spreadsheet or other application to build a table to implement an eVRF workbook. Ultimately, a software application specifically used for this purpose would offer the most flexible way to create and edit a visibility surface definition and coverage maps. See the *eVRF Guidebook* for more information [11].

6.8 TELEMETRY GENERATION AND PROCESSING

The quality and completeness of the visibility offered to cyber analysis is dependent upon the observation points and telemetry-generating system components. The following subsections outline what services agencies will need to use to ensure effective security visibility and management of cloud business applications. In implementing these services, agencies should comply with the logging requirements issued by OMB M-21-31 [4] and consult NIST Special Publication 800-92 [20] for additional guidance on security log management.[1] This will enable agencies to collect the logs they need for their own security operations and provide additional visibility to CISA.

6.8.1 Logging

Agencies will need to configure their cloud services—including holistic, independent cloud security capabilities—to generate logs for their applications to enable cybersecurity outcomes, which include improved visibility, asset management, incident response, and more. Cloud

[1] NIST is in the process of revising the NIST Special Publication 800-92 (https://csrc.nist.gov/Projects/log-management).

security capabilities, coupled with an artificial intelligence engine that can work both at the edge and in the cloud, can support monitoring and threat prevention efficiently by exploiting parallelism and at a lower cost. Logs are also essential to fulfill many compliance requirements. By leveraging the eVRF workbook for SCuBA, agencies can determine which necessary log data to collect to enable these outcomes and detect different TTPs, and which logs to share with CISA.

To ensure appropriate levels of visibility, agencies must collect logs from multiple observation points. Figure 9 presents an alternate SCuBA security and visibility view that emphasizes collecting telemetry and logs.

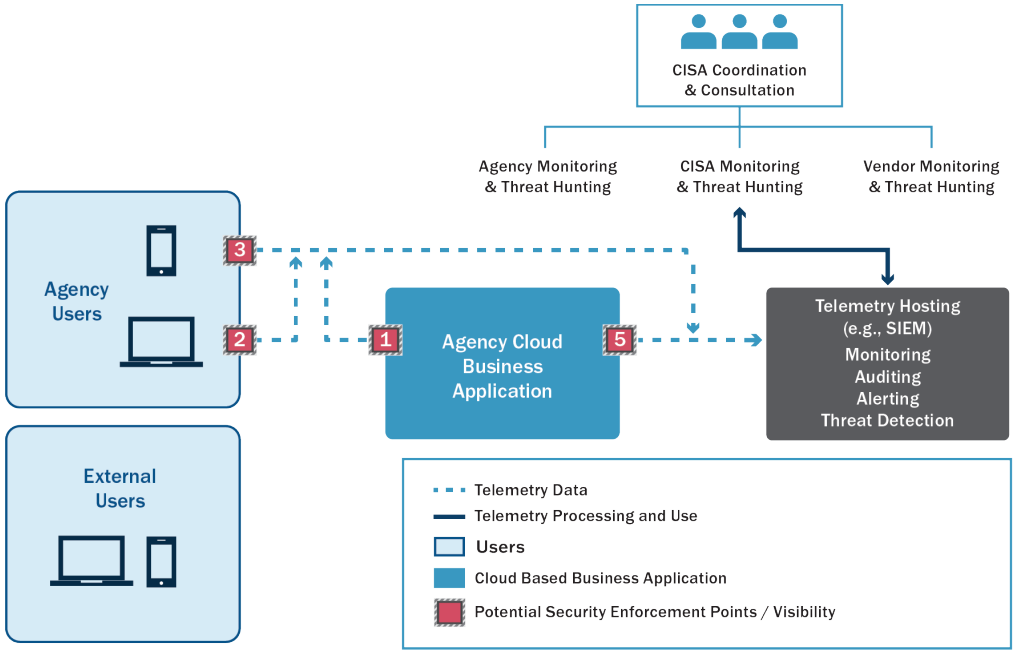

Figure 9. SCuBA telemetry

In cloud business applications, collect logs from each of the key building blocks previously identified:

- The SCA solution.
- The endpoint solution.
- The agency cloud business application.
- The security services, such as the ICAM solution (whether on-premises or cloud-based) and the secure DNS solution.

To facilitate analysts' needs and internal agency monitoring, auditing, alerting, and threat detection activities, aggregate the telemetry and logs as shown in Figure 9 via the agency's Telemetry Hosting solution, such as an agency's security information and event management (SIEM) solution. An eVRF visibility surface definition and OMB M-21-31 [4] logs should capture both key business events (e.g., send/receive email, document sharing outside of tenant, etc.) and configuration changes (e.g., new user creation, policy updates), as both can be indicative

of cybersecurity events. Generate logs in an automated manner. Configure logs to capture numerous pieces of contextual information regarding cloud activities, accesses, and resource states; this often includes fields or attributes such as associated user ID, resource ID, Application Programming Interface (API) name, timestamp, IP addresses, etc. The eVRF visibility surface definition identifies specific metadata in more detail. Agencies will need to manage issues associated with scaling, retention, access, privacy, provenance, exportability and timeliness—among other issues—of their logs and ensure that the logs shared with CISA in real time are properly delivered per the NCPS Cloud Interface RA [6], [7].

6.8.2 Monitoring

While record keeping and compliance purposes require storage of some logs, others will be monitored, audited, and analyzed as part of broader agency security posture management. Therefore, agencies should incorporate logs from their cloud business applications into their monitoring services to update tracking metrics, conduct resource mapping, and generate security reports, which will in turn facilitate auditing, alerting, and threat detection. The same applies for new security services deployed as part of SCuBA adoption. While log generation is essential for visibility, agencies should complete appropriate ongoing monitoring to maintain situational awareness and facilitate response actions.

6.8.3 Auditing

Agencies should further analyze their application logs and security reports through security auditing. This addresses various contextual questions for a potential event such as the users, processes, services, or applications involved; what was done; where it took place; when it occurred and over what time period; how it occurred; and the impact. All logs should use Network Time Protocol standards as prescribed by NIST guidance. Auditing services allow agencies to better understand what is happening within (and to) their cloud environments and ensure they are operating as desired. This is a more labor-intensive process than automated monitoring and report generation, as it typically involves a human policy decision point (as opposed to a technology policy decision point). Periodic audits further seek to discern not only whether given transactions occur, but whether they should occur in normal operating conditions and states. The additional review of organizational visibility (i.e., the awareness of business functions, priorities, risks, and collaboration agreements) enhances auditor precision and can provide further insights to an agency.

6.8.4 Alerting

Agencies should create alerts for their business applications that automatically generate based on their monitoring and auditing data. Alerts enable agencies to quickly identify various issues with business applications such as misconfigurations, unauthorized access, privilege changes, and other anomalous activities for review and remediation. Such alerts represent the result of defects or heuristically derived detections and deserve preferential treatment in analysis tools and dashboards (with respect to the raw data used to generate the alerts). Agencies should integrate these alerts into their existing security operations

center (SOC) procedures and leverage their existing SIEM and security automation, orchestration, and response (SOAR) tooling to respond to security alerts. Agencies should conduct regular testing and review alerts to ensure accuracy and timeliness metrics align with agencies' risk tolerances and support federal requirements.

6.8.5 Threat Detection

Agencies can leverage a variety of tools and services to detect and mitigate potentially malicious activity taking place within or against their cloud environments through business applications. Threats include denial of service, data exfiltration, malware injection, unauthorized privilege escalation and account creation, etc. Agencies may detect threats through automated means (artificial intelligence, machine learning, etc.) or manual discovery. Data visualization tools and dashboards assist agency analysts in detecting threats against agency cloud business applications. Agencies should review threat-detection services—either offered natively by their service provider, as a third-party offering that integrates with the native service, or as a stand-alone service—to incorporate anomaly detection, machine learning, threat intelligence, etc., within their threat detection capabilities for their cloud business applications. Agencies should test these services to benchmark fidelity in the alerts generated and latencies in detection. Agencies should also update their logging, monitoring, auditing, and alerting policies and procedures based on lessons learned from their threat detection capabilities and proactive threat hunting activities (e.g., to incorporate analytics for newly discovered threats, reduce false positives, and expand visibility coverage to mitigate gaps).

6.9 SHARED RESPONSIBILITY MODEL

The SCuBA TRA relies on a shared responsibility model, as shown in Figure 10 and described in the following subsections, between the agency, CISA, and the selected vendors. Each entity plays a critical role in ensuring a robust security posture and achieving the desired security outcomes. This is true both with respect to protective security controls and to visibility, detection, and response.

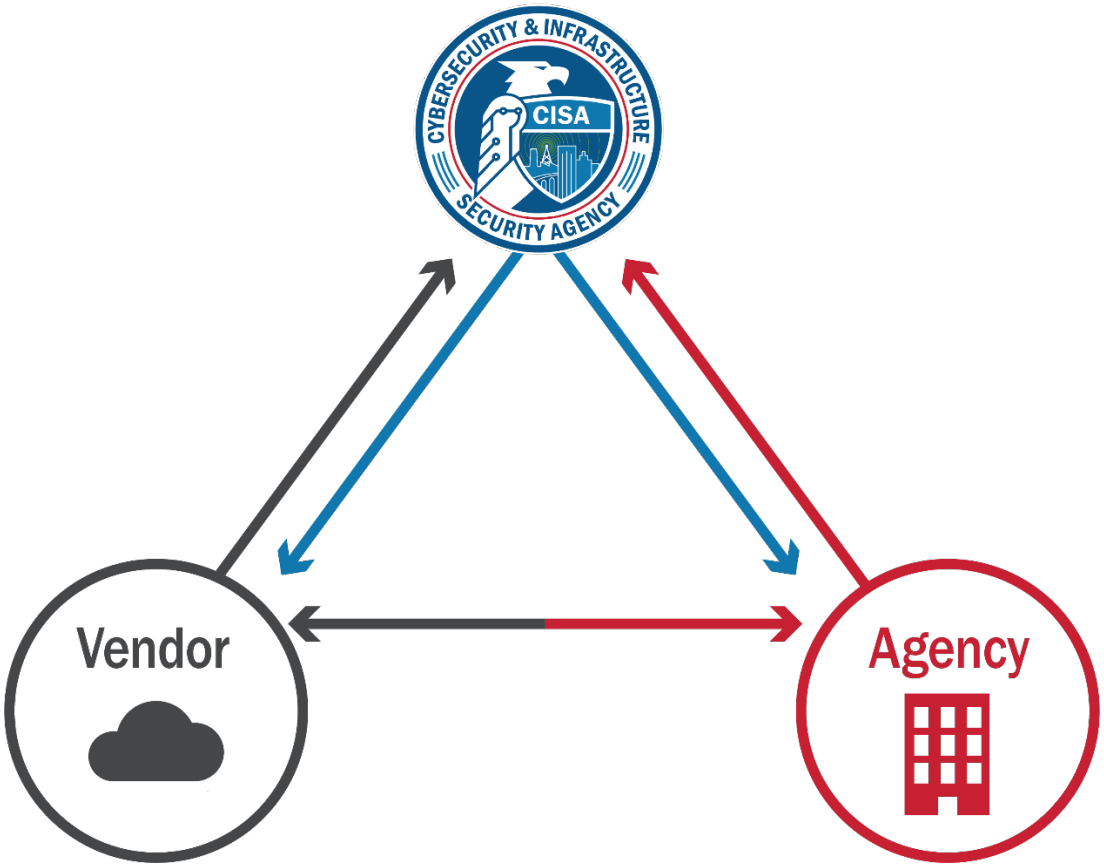

Figure 10. Shared responsibility model

6.9.1 Protective Security Controls and Services

Agencies: Agencies are responsible for properly configuring their chosen cloud business application platform in accordance with the SCuBA solution architecture documents. Agencies are also responsible for ensuring that their SCuBA deployment leverages appropriate capabilities of their other security services as discussed in Sections 6.1 and 6.5.

Vendors: Vendors are responsible for securing the underlying SaaS platform behind the business applications. Vendors should also offer agencies the necessary product capabilities to implement the required security controls, including integrations with independent software vendor solutions (e.g., to provide email security services or identity services), if necessary.

CISA: CISA is responsible for defining the baseline security requirements, architectures, and configurations necessary to realize the SCuBA vision. CISA is also responsible for developing shared services to implement pieces of the TRA (e.g., PES).

6.9.2 Visibility, Detection, and Response

Agencies: Agencies are responsible for first-line security operations, such as alert triage and response to limited-scope incidents. Agencies collect and retain logs per OMB M-21-31 and

CISA guidelines (both the CISA logging guidance and the eVRF CISA visibility requirements). Agencies can leverage CISA-provided shared services to enhance their logging and security monitoring operations. Agencies are also encouraged to coordinate with their vendors and/or service providers on the application of telemetry configuration and visibility coverage map generation, which may include feature requests in future product releases or lead to enhanced integration with third-party offerings. Agencies should apply the eVRF concepts to their specific cloud business applications to generate appropriate logs, and should use the SCuBA security baselines to ensure relevant security controls are enforced. These activities will further CISA's support for federal agencies.

Vendors: Cloud business application providers can share vulnerability and breach-related information with CISA and agencies to enhance situational awareness and facilitate response activities. Additionally, vendors can identify trends and threat activities across sectors and service offerings. They can respond to threats that are undetectable to their tenants and update their offerings to mitigate vulnerabilities and adversarial campaigns. Vendors can also share information regarding updates and changes to their products, share guidance on how to effectively use their offerings as engineered, and provide formal instruction and training opportunities to ensure consistent understanding of product limitations and features.

CISA: CISA's duties include refining visibility requests, updating baselines, and providing response support. One of CISA's primary responsibilities is to assist agencies in threat discovery and remediation. Therefore, CISA will engage with FCEB agencies to facilitate data acquisition of cloud logs and telemetry to ensure delivery aligns with CISA's preferences for timeliness, frequency, format, and other attributes as described in the *National Cybersecurity Protection System Cloud Interface Reference Architecture Volume Two: Reporting Pattern Catalog* [7]. This telemetry will enable CISA's analysis, incident response, and threat hunting activities. CISA will engage cloud vendors to mitigate security and visibility gaps providing enhanced security for cloud business applications. CISA will also coordinate with cloud vendors to mitigate risks facing FCEB agencies' cloud services through information sharing and the deployment of security services.

7. CONCLUSION

The SCuBA TRA provides context, standard views, and terminology that informs all SCuBA efforts and aligns them with higher level RAs such as the Cloud Security TRA CISA published. It provides guidance for FCEBs to develop their own cloud business applications. The SCuBA TRA will be updated as technological advances occur and as the program evolves.

8. References

[1] 117th Congress, "H.R. 1319 - American Rescue Plan Act of 2021," Senate and House of Representatives of the United States of America, Washington, D.C., 2021.Public Law 117-2.

[2] 116th Congress, H.R. 6395, National Defense Authorization Act for Fiscal Year 2021, Washington, D.C.: United States Congress, 2021. Public Law 116-283.

[3] CISA, United States Digital Service, and Federal Risk and Authorization Management Program, "Cloud Security Technical Reference Architecture," 2021. [Online]. Available: https://www.cisa.gov/cloud-security-technical-reference-architecture.

[4] Office of Management and Budget, "M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," 27 August 2021. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf. [Accessed 15 November 2021].

[5] Office of Management and Budget, "M-22-09: Moving the U.S. Government Towards Zero Trust Cybersecurity Principles," 26 January 2022. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf. [Accessed February 2022].

[6] CISA, "CISA NCPS Cloud Interface Reference Architecture Volume 1: General Guidance," Cybersecurity and Infrastructure Security Agency, Arlington, VA, 2020.

[7] CISA, "National Cybersecurity Protection System Cloud Interface Reference Architecture Volume Two: Reporting Pattern Catalog," Cybersecurity and Infrastructure Security Agency, Arlington, VA, 2020.

[8] CISA, "Trusted Internet Connections Guidance Repository," Cybersecurity & Infrastructure Security Agency (CISA), [Online]. Available: https://www.cisa.gov/tic-guidance. [Accessed February 2022].

[9] CISA, "Continuous Diagnostics and Mitigation CDM)," CISA CDM Program Management Office, [Online]. Available: https://www.cisa.gov/cdm. [Accessed January 2022].

[10] CISA, "CISA Blog on SCuBA," [Online]. Available: https://www.cisa.gov/blog/2022/03/31/secure-cloud-business-applications.

[11] CISA, "Extensible Visibility Reference Framework (eVRF) Program Guidebook--Request for Comment Draft," April 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/eVRF_Guidebook_RFC_508C.pdf. [Accessed August 2022].

[12] General Services Administration, "FedRAMP," [Online]. Available: https://www.gsa.gov/technology/government-it-initiatives/fedramp. [Accessed January 2022].

[13] "FEDRAMP Frequently Asked Questions," [Online]. Available: https://www.fedramp.gov/faqs/.

[14] General Services Administration (GSA), "Federal ICAM Architecture Introduction," IDManagement.gov, 6 January 2021. [Online]. Available: https://playbooks.idmanagement.gov/arch/. [Accessed January 2022].

[15] P. Grassi, M. Garcia and J. Fenton, "NIST Special Publication 800-63-3, Digital Identity Guidelines," June 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html. [Accessed November 2021].

[16] Office of Management and Budget, "M-22-01: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response," 8 October 2021. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf. [Accessed February 2022].

[17] CISA, "Continuous Diagnostics and Mitigation Program, Technical Capabilities, Vol 2: Requirements Catalog," Cybersecurity and Infrastructure Security Agency (CISA), Arlington, VA, 2020.

[18] CISA, "CISA Releases Capacity Enhancement Guides to Enhance Mobile Device Cybersecurity for Consumers and Organizations," Cybersecurity & Infrastructure Security Agency, 24 November 2021. [Online]. Available: https://www.cisa.gov/uscert/ncas/current-activity/2021/11/24/cisa-releases-capacity-enhancement-guides-enhance-mobile-device. [Accessed December 2021].

[19] CISA, "Applying Zero Trust Principles to Enterprise Mobility. (DRAFT)," Cybersecurty & Infrastructure Security Agency, Arlington, VA, Not released to date..

[20] National Institute of Standards and Technology (NIST), "NIST Guide to Computer Security Log Management," 13 September 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-92/final. [Accessed 15 November 2021].

[21] CISA , "Zero Trust Maturity Model," June 2021. [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model. [Accessed Jan 2022].

APPENDIX A. GLOSSARY

Application Programming Interface (API): A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Cloud service provider (CSP): An external company that provides a platform, infrastructure, applications and/or storage services for its clients.

Continuous Diagnostics and Mitigation (CDM): A CISA program that provides a dynamic approach to fortifying government networks and systems cybersecurity by delivering cybersecurity tools, integration services and dashboards that help participating agencies improve their security posture.

Domain Name System (DNS): A system that stores information associated with domain names in a distributed database on networks. DNS translates IP addresses into human-understandable names.

Enterprise mobility management (EMM): A suite of services and technologies that enables an agency to secure the use of mobile devices (e.g., tablets, smartphones, and e-readers) per the agency's policies. Components of an EMM include mobile device management, mobile application management, and mobile identity management.

extensible Visibility Reference Framework (eVRF): Defines the concepts, requirements, and mechanisms for CISA, FCEB agencies, and other partners to collect and apply cyber visibility to mitigate threats. eVRF was created in response to Executive Order 14028, "Improving the Nation's Cybersecurity."

Federal Civilian Executive Branch (FCEB): A subset of U.S. federal departments and agencies that excludes the Department of Defense and agencies in the intelligence community.

Identity, Credential and Access Management (ICAM): A fundamental and critical cybersecurity capability that ensures the right people and non-person entities (NPEs) have the right access to the right resources at the right time.

Internet Engineering Task Force (IETF): A large, open, international internet standards body comprised of network designers, operators, vendors and researchers interested in how the internet architecture evolves and the smooth operation of the internet. The IETF technical work of developing open standards through open processes is done in working groups that are organized by topic into several areas.

Secure cloud access (SCA): A subset of remote access solutions that provide the ability for a trusted user on a remote workstation to securely access the agency's business application on a cloud service provider.

Security information and event management (SIEM): An application used to gather security data from across systems to facilitate monitoring, analysis, triaging, and alerting through a single interface.

Security operations center (SOC): A centralized operations center for monitoring, analyzing, detecting, and responding to security information and security incidents.

Security orchestration, automation, and response (SOAR): A platform or collection of technologies for coordinating, defining, automating, and executing tasks to analyze and respond to security data and security incidents. This often includes threat and vulnerability management technologies, security incident response capabilities, and additional tools that enable automation across security operations.

Software- s a service (SaaS): The capability provided to the consumer to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Technical Reference Architecture (TRA): A document that illustrates recommended approaches to cloud migration and data protection, as outlined in Section 3(c)(ii) of Executive Order 14028. As the federal government continues to transition to the cloud, the TRA will be a guide for agencies to leverage when migrating to the cloud securely. Additionally, the document explains considerations for shared services, cloud migration and cloud security posture management.

Telemetry: Artifacts derived from security capabilities that provide visibility into security posture.

Zero Trust (ZT): Per Executive Order 14028, "the term ''ZT Architecture'' (ZTA) means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. In essence, a ZTA allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, ZT can ensure that the damage is contained. The ZTA security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity.

APPENDIX B. ABBREVIATIONS

Abbreviation	Definition
API	Application Programming Interface
ATT&CK	[MITRE] Adversarial Tactics, Techniques and Common Knowledge
CASB	Cloud access security broker
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CSP	Cloud service provider
DNS	Domain Name System
DoH	DNS over hypertext transport protocol secure
DoT	DNS over Transport Layer Security
E3A	EINSTEIN 3 Accelerated
EaaS	Environment as a service
EDR	Endpoint detection and response
EMM	Enterprise Mobility Management
eVRF	extensible Visibility Reference Framework
FCEB	Federal Civilian Executive Branch
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential and Access Management
GSA	Government Services Administration
GWS	Google Workspace
IaaS	Infrastructure as a service
ICAM	Identity, credential and access management
IDaaS	Identity as a service
IETF	Internet Engineering Task Force
IOA	Indicators of attack
IOC	Indicators of compromise
IP	Internet protocol
IT	Information technology
M365	Microsoft 365
MFA	Multi-Factor Authentication
NCPS	National Cybersecurity Protection System

Abbreviation	Definition
NIST	National Institute of Standards and Technology
NPE	Non-person entity
OMB	Office of Management and Budget
PaaS	Platform as a service
PES	Protective email services
pDNS	Protective Domain Name System
PIV	Personal identity verification
RA	Reference Architecture
SaaS	Software as a service
SASE	Secure Access Service Edge
SCA	Secure cloud access
SCuBA	Secure Cloud Business Applications
SEG	Secure Email Gateway
SIEM	Security information and event management
SME	Subject matter expert
SOAR	Security automation, orchestration, and response
SOC	Security operations center
TIC	Trusted Internet Connection
TRA	Technical Reference Architecture
TTPs	Tactics, Techniques and Procedures
ZT	Zero trust
ZTA	Zero Trust Architecture
ZTMM	Zero Trust Maturity Model