TLP:CLEAR

Trusted Internet Connections 3.0

Remote User Use Case

April 2023
Version 2.0
Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

REVISION HISTORY

The version number will be updated as the document is modified. This document will be updated as needed to reflect modern security practices and technologies.

Table 1: Revision History

Version	Date	Revision Description	Section/Page Affected
Draft	December 2020	Initial Release	All
1.0	October 2021	Response to RFC and Stakeholder Feedback	All
		New Universal Security Capability for User Training and Awareness Added	Pg. 24
2.0	April 2023	Added 5 Universal Security Capabilities: Supply Chain Risk Management; Resource Lifecyle Management; Security Test and Exercise; Continuous Monitoring Reporting; Governance and Policy Auditing	Pg. 25-27
		Added 11 Email PEP Security Capabilities: Sender Denylisting; Post-Delivery Protections; Malicious File Protections; Adaptive Email Protections; Email Labeling; User Tipping, Content Filtering; User Digital Signatures for Outgoing Email; Encryption for Outgoing Email; Mail Content Query; and Email Domain Reputation Protections	Pg. 31-33
		Updated definition of Web PEP Security Capability: Domain Resolution Filtering	Pg. 35

Version	Date	Revision Description	Section/Page Affected
		Added 1 Networking PEP Security Capability: Resource Containment	Pg. 40
		DNS PEP Security Capability: - Added CISA's Protective DNS Service - Removed EINSTEIN 3 Accelerated Domain Name Protections	Pg. 42
		Added 1 Intrusion Detection PEP Security Capability: Network Detection and Response	Pg. 43
		Added 4 Unified Communications and Collaboration PEP Security Capabilities: Anti-phishing Protections; Malicious Link Protections; Link Click-through Protections; and Malicious File Protections	Pg. 47-48
		Added 2 Data Protection PEP Security Capabilities: Data Labeling, and Data Inventory	Pg. 50
		Added 7 Identity PEP Security Capabilities: Adaptive Authentication; Entitlement Inventory; Secrets Management; Behavioral Baselining; Enterprise Identity and Access Management; Multi-factor Authentication; and Continuous Authentication	Pg.51-53
		Updated References	Throughout document
		Updated Appendix B	Pg. 58

This use case references *Trusted Internet Connections 3.0 Security Capabilities Catalog,* v3.0, dated April 2023. The applicable security capabilities will be further explained in the document. This document replaces and rescinds the *TIC 3.0 Interim Telework Guidance*.

READER'S GUIDE

The Trusted Internet Connections (TIC) initiative is defined through key documents that describe the directive, the program, the capabilities, the implementation guidance, and capability mappings. Each document has an essential role in describing TIC and its implementation. The documents provide an understanding of how changes have led to the latest version of TIC and why those changes have occurred. The documents go into high-level technical detail to describe the exact changes in architecture for TIC 3.0. The documents are additive; each builds on the other like chapters in a book. As depicted in Figure 1, the documents should be referenced in order and to completion to gain a full understanding of the modernized initiative.

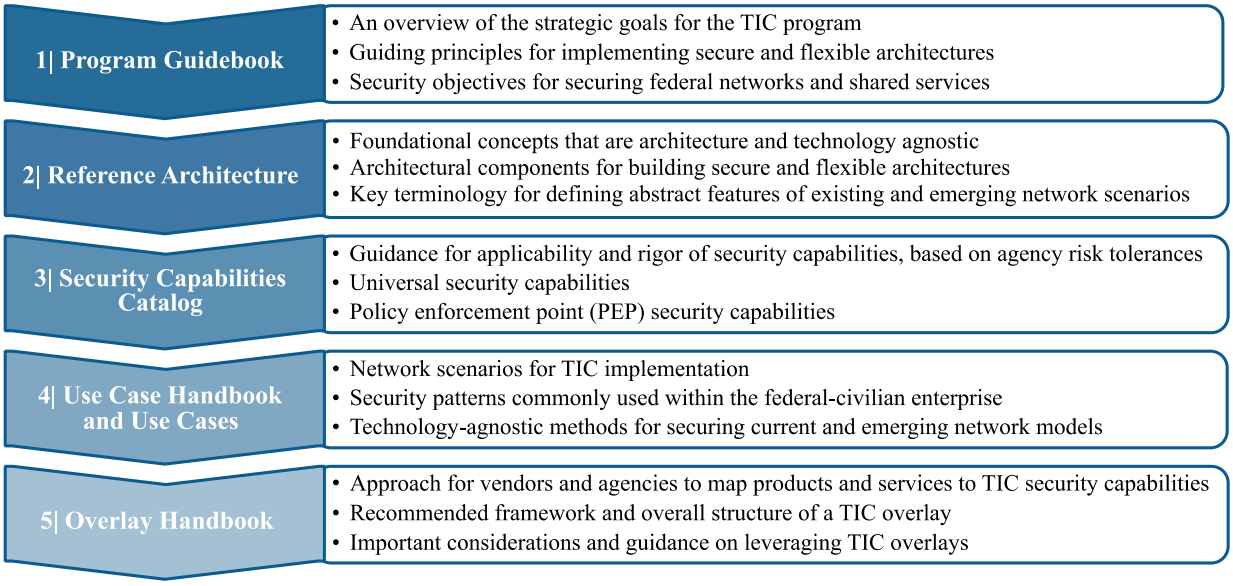


Figure 1: TIC 3.0 Guidance Snapshot

CONTENTS

Figures

Tables

1. INTRODUCTION

Trusted Internet Connections (TIC), originally established in 2007, is a federal cybersecurity initiative intended to enhance network and perimeter security across the Federal Government. The Office of Management and Budget (OMB), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the General Services Administration (GSA) oversee the TIC initiative through a robust program that sets guidance and an execution framework for agencies to implement a baseline perimeter security standard.

The initial versions of the TIC initiative sought to consolidate federal networks and standardize perimeter security for the federal enterprise. As outlined in OMB Memorandum (M) 19-26: *Update to the Trusted Internet Connections (TIC) Initiative*[1], this modernized version of the initiative expands upon the original to drive security standards and leverage advances in technology as agencies adopt mobile and cloud environments. The goal of TIC 3.0 is to secure federal data, networks, and boundaries while providing visibility into agency traffic, including cloud communications.

1.1 KEY TERMS

To avoid confusion, terms frequently used throughout the TIC 3.0 documentation are defined below. Some of these terms are explained in greater detail throughout the TIC 3.0 guidance. A comprehensive glossary and acronyms list with applicable attributions can be found in Appendix A.

Boundary: A notional concept that describes the perimeter of a zone (e.g., mobile device services, general support system (GSS), Software-as-a-Service (SaaS), agency, etc.) within a network architecture. The bounded area must have an information technology (IT) utility.

Internet: The internet is discussed in two capacities throughout TIC documentation.

1. A means of data and IT traffic transport.
2. An environment used for web browsing purposes, hereafter referred to as "Web."

Managed Trusted Internet Protocol Services (MTIPS): Services under GSA's Enterprise Infrastructure Solutions (EIS) contract vehicle that provide TIC solutions to government clients as a managed security service. It is of note that the EIS contract is replacing the GSA Networx contract vehicle that is set to expire in Fiscal Year (FY) 2023.

Management Entity (MGMT): A notional concept of an entity that oversees and controls security capabilities. The entity can be an organization, network device, tool, service, or application. The entity can control the collection, processing, analysis, and display of information collected from the policy enforcement points (PEPs), and it allows IT professionals to control devices on the network.

Policy Enforcement Point (PEP): A security device, tool, function, or application that enforces security policies through technical capabilities.

Security Capability: A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).[2] Security capabilities help to define protections for information being processed, stored, or transmitted by information systems.

---

[1] "Update to the Trusted Internet Connections (TIC) Initiative," Office of Management and Budget M-19-26 (2019). https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf.
[2] "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R5)," December 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

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

TIC: The term "TIC" is used throughout the Federal Government to denote different aspects of the TIC initiative; including the overall TIC program, a physical TIC access point (also known as a Traditional TIC), and a TIC Access Provider (TICAP – see below). This document refers to TIC as an adjective or as the Trusted Internet Connections initiative.

TIC Access Point: The physical location where a federal civilian agency consolidates its external connections and has security controls in place to secure and monitor the connections.

TIC Access Provider (TICAP): An agency or vendor that manages and hosts one or more TIC access points. Single Service TICAPs serve as a TIC Access Provider only to their own agency. Multi-Service TICAPs also provide TIC services to other agencies through a shared services model.

TIC Overlay: A mapping of products and services to TIC security capabilities.

TIC Use Case: Guidance on the secure implementation and/or configuration of specific platforms, services, and environments. A TIC use case contains a conceptual architecture, one or more security pattern options, security capability implementation guidance, and CISA telemetry guidance for a common agency computing scenario.

Trust Zone: A discrete computing environment designated for information processing, storage, and/or transmission that share the rigor or robustness of the applicable security capabilities necessary to protect the traffic transiting in and out of a zone and/or the information within the zone.

Web: An environment used for web browsing purposes. Also see Internet.

2. OVERVIEW OF THE TIC USE CASES

TIC use cases provide guidance on the secure implementation and configuration of specific platforms, services, and environments, and will be released on an individual basis. The guidance is derived from pilot programs and best practices from the public and private sectors. The purpose of each TIC use case is to identify the applicable security architectures, data flows, and policy enforcement points (PEPs) and to describe the implementation of the security capabilities in a given scenario. TIC use cases articulate:

- Network scenarios for TIC implementation,
- Security patterns commonly used within the federal civilian enterprise, and
- Technology-agnostic methods for securing current and emerging network models.

TIC use cases build upon the key concepts and conceptual implementation of TIC 3.0 presented in the *TIC 3.0 Reference Architecture* (Reference Architecture) and provides implementation guidance for applicable security capabilities defined in the *TIC 3.0 Security Capabilities Catalog* (Security Capabilities Catalog). The *TIC 3.0 Use Case Handbook* (Use Case Handbook) provides general guidance for how agencies can utilize and combine use cases.

Agencies have flexibility in implementing TIC use cases. In particular:

- An agency may combine one or more use cases to best design and implement their TIC architectures.
- Use cases may provide more than one option for implementing a security pattern in order to give agencies flexibility.

- Each trust zone in a use case will be labeled with a notional high, medium, or low trust level, based on a pilot implementation or best practice. The use cases are depicted following the schema illustrated in Figure 2. Agencies can modify this trust zone designation to meet their needs and reflect their environment, including assigning a zone to a different trust level or altering the number of trust levels and their labels. Refer to the Reference Architecture for more details on trust zones.

Figure 2: Use Case Trust Zone Legend

- When securing trust zones, agencies should consider unique data sensitivity criteria and the impact of compromise to agency data stored in trust zones. Agencies may apply additional security capabilities that have not been included in the use case.
- Agencies have the discretion to determine the level of rigor necessary for applying security capabilities in use cases, based on federal guidelines and their risk tolerance.

Refer to the Use Case Handbook for more information on TIC use cases.

3. PURPOSE OF THE REMOTE USER USE CASE

The *TIC 3.0 Remote User Use Case* (Remote User Use Case) defines how network and multi-boundary security should be applied when an agency permits remote users on their network. A remote user is an agency user that performs sanctioned business functions outside of a physical agency premises. The remote user scenario has two distinguishing characteristics:

1. Remote user devices are not directly connected to network infrastructure that is managed and maintained by the agency.
2. Remote user devices are intended for individual use (i.e., not a server).

In contrast, when remote user devices are directly connected to local area networks and other devices that are managed and maintained by the agency, it would be considered either an agency campus or a branch office scenario. TIC architectures for agency campus and branch office scenarios are enumerated in the *TIC 3.0 Traditional TIC Use Case* (Traditional TIC Use Case) and the *TIC 3.0 Branch Office Use Case* (Branch Office Use Case) respectively.

Typical examples of remote users include personnel working from home, connecting from a hotel, or telecommuting from a non-agency-controlled location. For this use case, remote users will also include individuals using mobile devices (e.g., smartphones and tablets). Even though these devices may physically be onsite (at a branch office or agency campus), devices would be considered remote user devices if they use an alternative method to obtain connectivity (e.g., cellular provider) rather than directly connecting to internal agency networks. Such devices would also include any personally owned devices used under a Bring Your Own Device (BYOD) policy. With respect to devices owned and managed by the agency which are sometimes directly connected to the network (e.g., laptops), agencies may use a combination of use cases as appropriate if policy enforcement parity is maintained.

The Remote User Use Case helps agencies preserve security while they gain application performance (e.g., latency, throughput, jitter, etc.); reduce costs through reduction of private links; and improve user experience by facilitating remote user connections to agency-sanctioned cloud services and internal agency services as well as supporting additional options for agency deployment. This use case is also intended to support policy enforcement parity for devices and connectivity options.

This use case includes three network security patterns:

- Secure remote user access to agency campus,
- Secure remote user access to agency-sanctioned cloud service providers (CSPs), and
- Secure remote user access to web.

An agency may implement a subset of these security patterns and not necessarily all three. For instance, an agency may not yet have agency-sanctioned cloud services with authorized direct connectivity from a remote user. In cases like these, the agency may only implement the remote user to web and remote user to agency campus security patterns.

Agencies may implement **additional security patterns** not covered in the Remote User Use Case.

Agencies may implement additional security patterns. These additional security patterns may be in scope for a different use case but would be out of scope of the Remote User Use Case.

4. ASSUMPTIONS AND CONSTRAINTS

This section outlines guiding assumptions and constraints for the Remote User Use Case. It is intended to clarify significant details about the construction and replication of this use case. The assumptions are broken down by the use case as a whole and by the unique entities discussed in the use case:

- Agency campus,
- Remote users,
- Agency-sanctioned CSPs, and
- Web.

The following are the assumptions and constraints of this use case.

- Requirements for information sharing with CISA in support of National Cyber Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM) purposes are beyond the scope of this document. Consult the NCPS program[3] and CDM program[4] for further details.
- This document assumes that due diligence is done to manage endpoints, therefore requirements for endpoint protection are beyond the scope of this document. Consult the Federal Information Security Modernization Act of 2014 (FISMA) or National Institute of Standards and Technology (NIST) references in Appendix B for additional guidance on endpoint protections, BYOD, and telework security.
- The TIC security capabilities applicable to the use case are not dependent on a particular data transfer mechanism. In other words, the same capabilities apply if the conveyance is over leased lines, software virtual private network (VPN), hardware VPN, etc.

[3] "National Cybersecurity Protection System," Cybersecurity and Infrastructure Security Agency. https://cisa.gov/national-cybersecurity-protection-system-ncps.
[4] "Continuous Diagnostics and Mitigation," Cybersecurity and Infrastructure Security Agency. https://cisa.gov/cdm.

- To avoid redundancy, the security patterns presented in the Remote User Use Case focus primarily on the initial connection from the remote user to an adjacent trust zone. Additional patterns can be constructed by combining security patterns from this use case with patterns from other use cases if policy enforcement parity is maintained. For example, Security Pattern 1 in this use case covers remote user access to agency on-premises services, of which a virtual desktop infrastructure (VDI) would be one example. The VDI may then be employed to access other services using any security patterns from the Traditional TIC Use Case.
- The scope of the Remote User Use Case is focused on network security. While this use case can be compatible with zero trust, implementation of zero trust requires additional controls and measures beyond those detailed in this use case, particularly with respect to those endpoints already inside the network perimeter.

The following are assumptions about the agency campus.

- For this use case, the agency campus entity may refer to the agency campus, branch office, or both.
- The agency campus utilizes the Traditional TIC Use Case, or equivalent security architectures, to access the web and CSPs.
- Any branch offices utilize the Branch Office Use Case, or equivalent security architectures, to access the web, CSPs, and the agency campus.
- The agency maintains control over and has significant visibility into the agency campus.
- Data is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.
- The agency employs network operation center (NOC) and security operation center (SOC) tools capable of maintaining and protecting their portions of the overall infrastructure. To accomplish this, agencies can opt to use a NOC and SOC, or commensurate solutions.

The following are assumptions about remote users.

- The remote user may be using either government furnished equipment (GFE) or BYOD.
- For GFE, remote users may be permitted business only use of their devices (e.g., Corporate-Owned Business Only (COBE)), or permitted for personal use (e.g., Corporate-Owned Personally Enabled (COPE)).
- Devices employed by remote users may include desktops, laptops, and mobile devices (e.g., smartphones and tablets). While remote users may connect to virtual desktop instances hosted by the agency or in cloud service providers, these agency-managed desktop instances are not considered remote user devices. However, they may be considered as agency virtual GFEs inside an agency campus or cloud environment.
- For GFE, the agency maintains control over and has significant visibility into devices used by the remote user. All traffic from GFE devices is in scope for TIC 3.0.
- For BYOD, the agency may have limited control and visibility into the device. Traffic from BYOD to the agency campus and to agency-sanctioned CSPs is in scope for TIC 3.0. While traffic to the web from BYOD is generally out of scope for TIC 3.0, if traffic to the web originates from an application accessing agency data, then the traffic would be in scope for TIC 3.0. Guidance on BYOD policies is beyond the scope of this document.
- Traditionally, the remote user would have used the agency campus for all CSP and web traffic.

- Agency data on remote user devices, or in transit to and from them, is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.
- The agency employs NOC and SOC tools capable of protecting remote user sessions. These functions may be performed as an extension to the NOC and SOC tools managed and housed at the agency campus or via commensurate solutions.

The following are assumptions about agency-sanctioned CSPs.

- CSPs are compliant with the Federal Risk and Authorization Management Program (FedRAMP).[5]
- Interactions with CSPs follow agency-defined policies and procedures for business need justification, partner connection eligibility, service levels, data protections, incident response information sharing and reporting, costs, data ownership, and contracting.
- The agency maintains awareness of which CSPs and CSP services are sanctioned for use by the agency. This awareness limits approved services to those which fulfill agency needs and have security consistent with agency risk tolerances.
- The agency has limited control over and visibility into CSP environments.
- CSPs have NOCs and SOCs that control and protect the portions of the service infrastructure where the agency has little or no control or visibility.
- The agency only uses secure mechanisms (e.g., transport layer security (TLS) or VPN) for CSP service administration.
- The agency only uses strong authentication mechanisms (e.g., Federal Information Processing Standard (FIPS) 140-3[6] compliant multi-factor authentication (MFA) for CSP service administration.
- Data stored at CSPs is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.
- CSPs allow the agency to define and/or configure policies that the CSP applies on their behalf.
- CSPs allow the agency to define roles and responsibilities for the definition and configuration of policies applied on their behalf by the CSP.
- CSPs provide the agency with mechanisms for obtaining visibility into the current state and history of the system (e.g., log information, configuration, accesses, system activity, etc.).
- CSPs provide commensurate protections and policy enforcement for traffic between the agency tenant and other tenants of the CSP as between the agency tenant and parties outside the CSP.

The following are assumptions about the web.

- The web contains untrusted entities.
- The agency can only apply policy to remote user resources for web access but has no ability to apply policy in the web or to web resources.

[5] "FedRAMP," General Services Administration (2019). https://www.fedramp.gov/federal-agencies/.
[6] "Security Requirements for Cryptographic Modules," National Institute of Standards and Technology (2019). https://csrc.nist.gov/publications/detail/fips/140/3/final.

5. CONCEPTUAL ARCHITECTURE

The Remote User Use Case focuses on the scenario in which an agency user performs business functions, either agency-hosted or in cloud environments, on the web or from outside agency network boundaries. Traditionally, when accessing these resources, agency users would first establish a trusted connection (e.g., VPN) to an agency campus, and then use this channel to access either agency-hosted or external resources.

As shown in Figure 3, this use case is composed of four trust zones: remote user, agency campus, CSP, and web. To simplify the visualization and descriptions, this use case shows a single remote user, and a single CSP trust zone. However, this simplification is not meant to imply that an agency must treat all remote users or all CSPs in the same manner. Applicable TIC capabilities and their rigor should be tailored for the nature of the remote user or the CSP service in use.

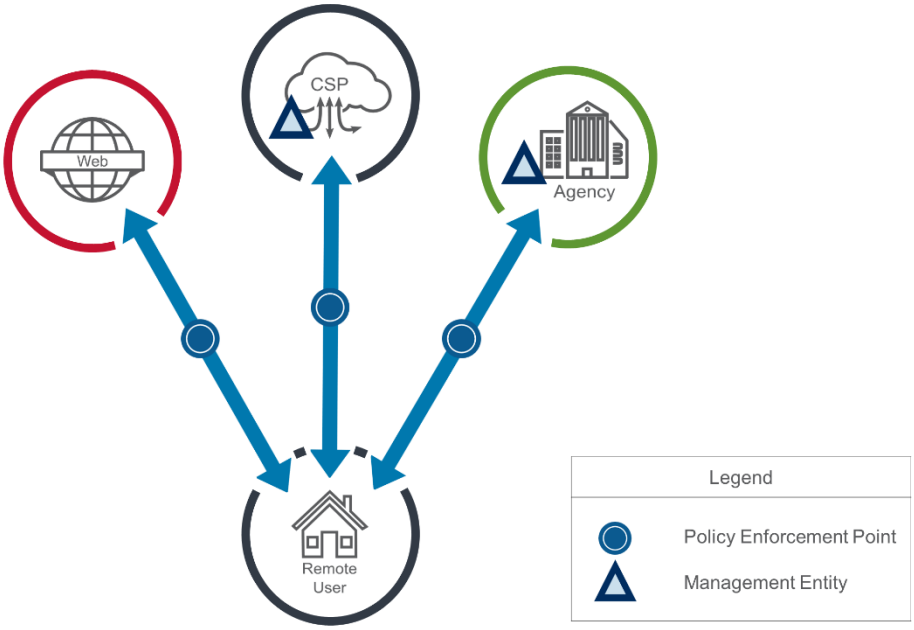


Figure 3: Remote User Conceptual Architecture

The trust zones depicted in Figure 3 are detailed in Table 2. The trust zones are labeled with levels of trust, using the example trust levels—high, medium, and low—explained in the Reference Architecture. While these levels were selected based on existing pilots or deployments, they may not capture the needs or requirements of all agencies. Agencies may determine and label trust zones according to the trust levels that best describe their environment. For example, an agency may have remote users that employ unmanaged personal devices and may decide to label that class of remote users with a lower trust level. Alternatively, an agency might decide to designate a CSP with a higher trust level based on agency criteria (e.g., the accreditation level of the CSP, the control and visibility, available protections, etc.).

Implementation Consideration

The trust levels in this use case are intended to be examples. Agencies may define and assign trust levels to align with their requirements, environments, and risk tolerance.

Table 2 briefly explains why each entity is labeled with either a high, medium, or low trust zone level in this use case to help agencies determine what is most appropriate in their implementation.

Table 2: Trust Zones in the Remote User Use Case

Trust Zone	Description
Remote User Trust Zone	The Remote User Trust Zone is a logical trust zone representing a device employed by a remote user when accessing agency resources. Remote user devices may be agency-managed (e.g., GFE) or not managed by agencies (e.g., BYOD). Devices not managed by agencies may not be suitable for performing some policy enforcement capabilities. The agency may have more limited control over and visibility into these devices. The Remote User Trust Zone is labeled with a ***medium trust level*** in this use case.
Agency Campus Trust Zone	The Agency Campus Trust Zone is the logical zone for the agency campus or the agency's enterprise network. The trust zone includes management entities (MGMTs) such as the NOC, SOC, and other entities. The agency maintains control over and visibility into the agency campus. It is responsible for defining policies, implementing them in the various PEPs controlled by the agency, and identifying and responding to incidents. Policy enforcement between the agency campus and the remote user could include various controls associated with the remote user establishing a trusted connection to the agency campus, as well as other services to secure the traffic to and from agency resources. The agency campus accesses external entities through the Traditional TIC Use Case, or equivalent, when accessing external entities or when transmitting traffic from the remote user to external entities. The Agency Campus Trust Zone is labeled with a ***high trust level*** in this use case.
Cloud Service Provider Trust Zone	The Cloud Service Provider Trust Zone is a logical trust zone for the CSP providing Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, or a similar service. The agency has limited control over and visibility into the CSP environment, with the CSP responsible for protecting the underlying cloud infrastructure and the agency providing certain policy-defined functions and capabilities. The trust zone includes a MGMT that executes locally scoped functions for the CSP environment. The Cloud Service Provider Trust Zone is labeled with a ***medium trust level*** in this use case.
Web Trust Zone	The Web Trust Zone is a logical trust zone that depicts an environment with untrusted external resources, including non-agency-sanctioned cloud service providers, where neither the agency nor entities acting on its behalf, may

Trust Zone	Description
	deploy or enforce policies. Given these limitations, the Web Trust Zone is labeled with a ***low trust level*** in this use case.

5.1 RISKS AND DEPLOYMENT CONSIDERATIONS

Traditional on-premises deployments often engage protections and policies for agency user devices that depend, in part, on their being on-premises. While these protections and policies may not protect against compromised on-premises entities, they are often used as part of an overall defense-in-depth strategy to reduce an agency's attack surface and the impact of compromise by:

- Limiting the types of devices agency users employ;
- Limiting the acquisition mechanisms and channels used for device procurement;
- Limiting the access to those devices;
- Limiting those devices' access to agency data, agency services, and external services; and
- Allowing access to the devices by system administrators and security analysts.

However, with agency users working outside the traditional agency physical and network boundaries, agencies may need to reconsider their deployed protections.

5.1.1 Physical Access Protections

Traditional on-premises deployments give agencies a myriad of options to scale the physical protection of agency user devices according to agency needs. Agencies can control where the devices are located and who has access to those locations, helping to limit the opportunity for theft, data loss, and tampering.

Beyond limiting the access of people to the devices, an on-premises deployment can be tailored to limit the types of peripherals that users can connect to their devices. Options can be provided to users for scanning or printing agency data, portable thumb drives to transfer data between agency user devices, and physical devices for agency users to back up their data if needed. When agency users are in a remote location, users may need to handle these tasks without access to agency deployed and managed peripherals, often leading to workarounds that may present risks.[7]

Remote user devices can also present challenges for agency NOC operators and SOC analysts. There are many situations in which an agency NOC operator or SOC analyst may need access to an on-premises device. In a traditional on-premises deployment, the device can be easily retrieved, facilitating incident response or device returns when no longer used. However, for remote user devices, agencies can no longer rely on the same level of access to the devices.

5.1.2 Network Protections

On-premises deployments limit the networks that agency user devices connect through. This allows them to ensure a baseline level of security protections that are independent of the device itself.

[7] See the CISA Printing While Working Remote Capacity Enhancement Guide for more information: https://www.cisa.gov/publication/capacity-enhancement-guides-federal-agencies.

These protections can limit the avenues available for attackers to harm the devices and their ability to exfiltrate data from the devices, permitting agencies to deploy fewer controls onto the endpoint devices themselves.

However, when users are working remotely, agencies can no longer rely on these network protections. Remote users are often connected to untrusted networks, whether in their home, at hotels, or on other public networks, that are also used by non-agency user devices and often have minimal security protections in place. While VPNs can mitigate some of these issues, their use is often mandated by policy and can be easily bypassed. Agency user devices' access to untrusted networks can also affect data exfiltration as the data may be exfiltrated over the untrusted network without impediment.

The use of untrusted networks can also affect how agency services are deployed. In a traditional on-premises environment, the agency has a greater understanding of where agency users are connecting from, which informs their deployment of protections around the services and data. However, when agency users are coming from unknown locations and untrusted networks, the agencies should reconsider the types of security controls placed around the services and data.

5.1.3 Device Diversity

In a traditional on-premises deployment, agencies can more easily limit the diversity of devices used to access agency services and data, simplifying the standardization of security controls that are applied. However, when an agency is looking to allow remote users, it is often necessary to allow more types of authorized devices to better facilitate remote users' ability to work effectively. Agencies may be able to deploy capabilities to remote users' devices, but the types of capabilities that can be deployed, and the rigor with which they can be deployed and enforced, may be limited by the breadth of devices that remote users use and the level of control that agencies have over their configuration.

5.1.4 Policy Enforcement Location

The security posture of agency user devices changes when the agency user is working outside the agency network. This may lead an agency to rethink the locations where security policies are enforced. In a traditional on-premises environment, agencies retain significant control and visibility into agency user devices, and these devices can support rigorous enforcement of agency policies. Under these conditions, agencies' risk tolerances might allow the deployment of capabilities to the agency user devices, grant the agency users more direct access to agency services, and allow the devices a greater ability to retrieve, process, and store agency data. However, as depicted in Figure 4, as this control and visibility of agency user devices decreases, agencies may look to move these capabilities further upstream from the endpoints, closer to the services or data.

Agencies may need to deploy additional capabilities to further restrict the types of access the agency user devices have to agency services and data. The agency must have policies in place ensuring that agency data is properly separated from personal data and cannot be accessed or transmitted except by agency-approved mechanisms.

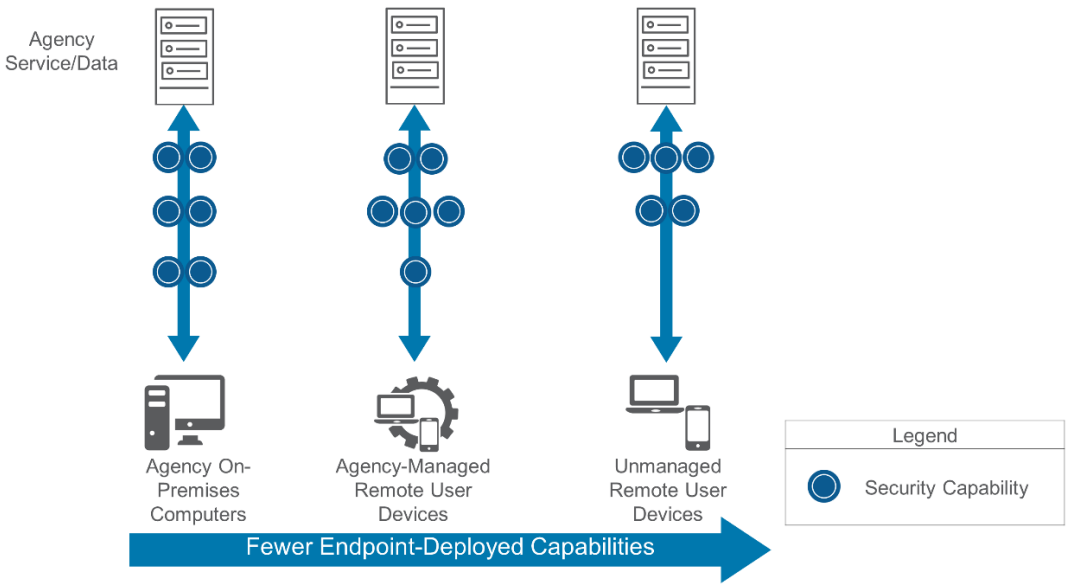


Figure 4: Notional Capability Deployment Locations by Agency Control and Visibility

5.2 AGENCY SERVICES CONNECTIVITY CONSIDERATIONS

Remote users commonly use three methods of accessing services, whether hosted by an agency or in a cloud environment. These methods, however, affect the control an agency has over the devices that access agency services and the layers of protection that are in place.

- **Direct Connection:** For services made available over the internet, the remote user may connect directly to the service. To control this access, these services often have a myriad of protections that are applied whether the access is coming from the internet or from inside the agency environment.
- **Virtual Private Network:** As a means of limiting access to agency services, remote users traditionally connect from a VPN into the agency and access the services through that connection. The services could then have access restricted to only connections through the VPN. To access cloud-hosted services, some agencies allow remote users to connect from a VPN directly to the CSP hosting the service. The remote user device is connected to the agency network, and all programs and services running on the remote user device may communicate with agency resources. Agencies often deploy protections between the remote user device and the agency network and services as well as on the remote user device itself. However, even with these protections, the remote user device still has substantial direct access to the agency environment and its services.
- **Remote Desktop Access:** The remote user can connect to an agency-managed desktop instance, possibly through an established VPN connection, and use applications on that desktop instance to access agency services. While similar to a traditional VPN, the remote user's use of a desktop instance, deployed and managed by the agency, more directly constrains the access of the remote user device to a well-defined and managed set of programs, ports, and services when accessing the agency environment and its services.

6. SECURITY PATTERNS

Three security patterns capture the data flows for the Remote User Use Case. Each of these has distinct sources, destinations, and options for policy enforcement. Regardless of the options chosen, due diligence must be practiced ensuring agencies are protecting their information in line with their risk tolerances, especially in instances where security policies are being applied by a third party on an agency's behalf, or in locations outside the agency's traditional sphere of control. In cases where additional security capabilities are necessary to manage residual risk, agencies should apply the controls or explore options for compensating capabilities that achieve the desired protections to manage risks. The security patterns include the following trust zone destinations:

- Agency campus,
- CSP, and
- Web.

The trust levels in these security patterns may not align with agency understanding of their environment, and as such agencies may determine and label trust zones according to those that best describe their environment.

6.1 SECURITY PATTERN 1: REMOTER USER TO AGENCY CAMPUS

This security pattern details the scenario where remote users are accessing resources that fall within the agency trust zone (e.g., agency campus, VPN, VDI, etc.). Options in this security pattern may be relevant to other security patterns that access external entities through the agency.

Four options are available for this connectivity and are outlined in Figure 5. Agencies may apply different constraints on connectivity options to different agency-hosted resources. Since the agency defines policies for both sides of the connection, the agency can determine the level of rigor for security capabilities to apply to traffic between the two trust zones, accounting for the limited control that the agency may have over the remote user's device. Due diligence must be practiced to ensure the agency is protecting its information in line with its risk tolerances and federal guidelines.

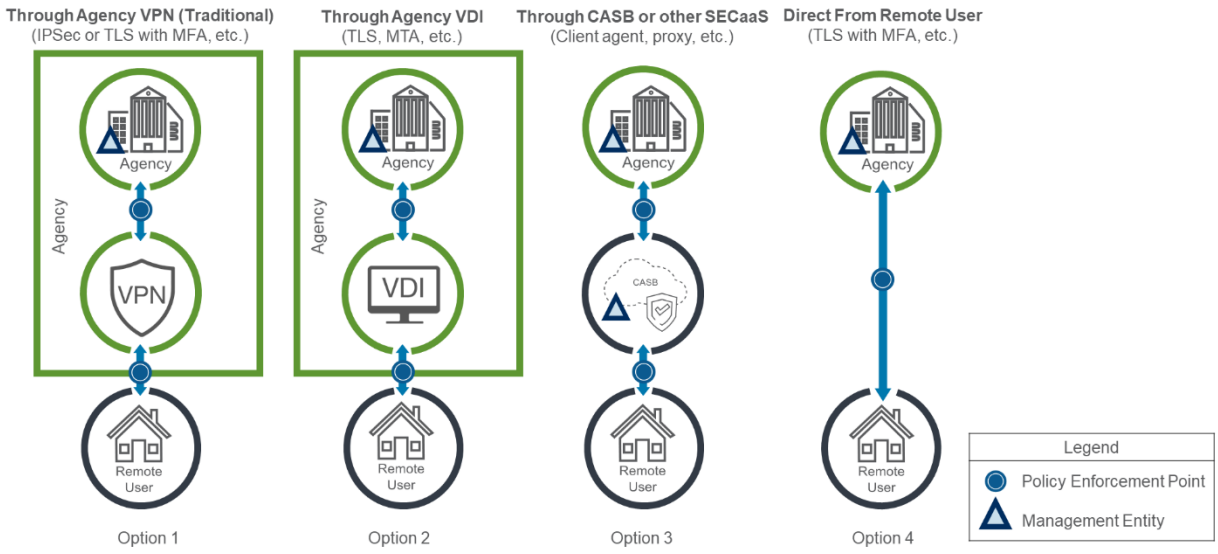
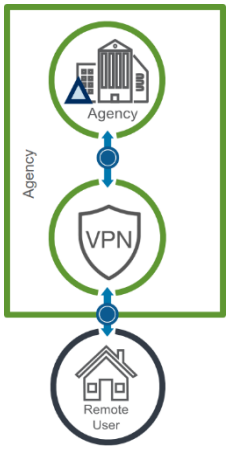
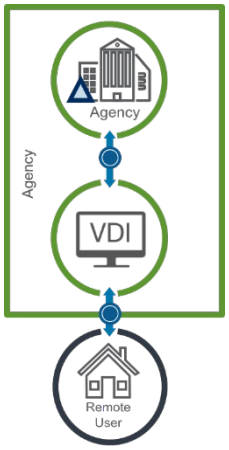


Figure 5: Security Pattern 1: Remote User to Agency Campus



In the **first option** (left), the remote user establishes a protected VPN connection to the agency campus to access agency-hosted resources. Policy enforcement placement and protections may be applied at the agency campus and, if possible, on the remote user's device. Multiple programs, ports, and protocols can utilize this same conveyance protection with shared protections.



In the **second option** (left), the remote user connects to an agency-managed desktop instance, either virtual or physical, located at the agency trust zone and uses that desktop instance to access agency-hosted resources. Policy enforcement placement and protections are commonly applied at desktop infrastructure and the agency campus. If possible, policy enforcement may also be applied on the remote user's device. Programs, ports, and protocols accessible to the remote user can be limited to only those required for VDI functionality.

The **third option** (left) permits connectivity from remote users to agency-hosted resources through a cloud access security broker (CASB) or other security-as-a-service (SECaaS) provider. Policy enforcement can be performed at the CASB, the agency campus, and, if possible, the remote user's device. Policy enforcement parity between the agency campus and remote users as well as other remote entities (e.g., branch offices) can be simplified when the locations use the same CASB or SECaaS provider. Remote users establish a protected connection to the CASB. Various methods can be used to direct remote user traffic to the CASB, including client agents, proxy settings, and domain name system (DNS) means. The CASB trust zone is labeled with a medium trust level in this option, though agencies may determine and label trust zones according to the trust levels that best describe their environment.

The **fourth option** (left) permits connectivity from remote users directly to resources on the agency campus via protected connections (e.g., TLS and MFA). Policy enforcement placement and protections are commonly applied at agency resource as well as the agency campus. If possible, policy enforcement may also be applied on the remote user's device. Policy enforcement parity between remote users and on-premises agency users can be simplified when protections are handled at the agency resource level and applied consistently no matter the location of the agency entity accessing the resource.

6.2 SECURITY PATTERN 2: REMOTE USER TO CLOUD SERVICE PROVIDER

Figure 6 illustrates the security pattern where an agency allows remote users to access resources within agency-sanctioned CSP environments. Three options for this connectivity are outlined below. Agencies may apply different constraints on connectivity options to different CSP resources.

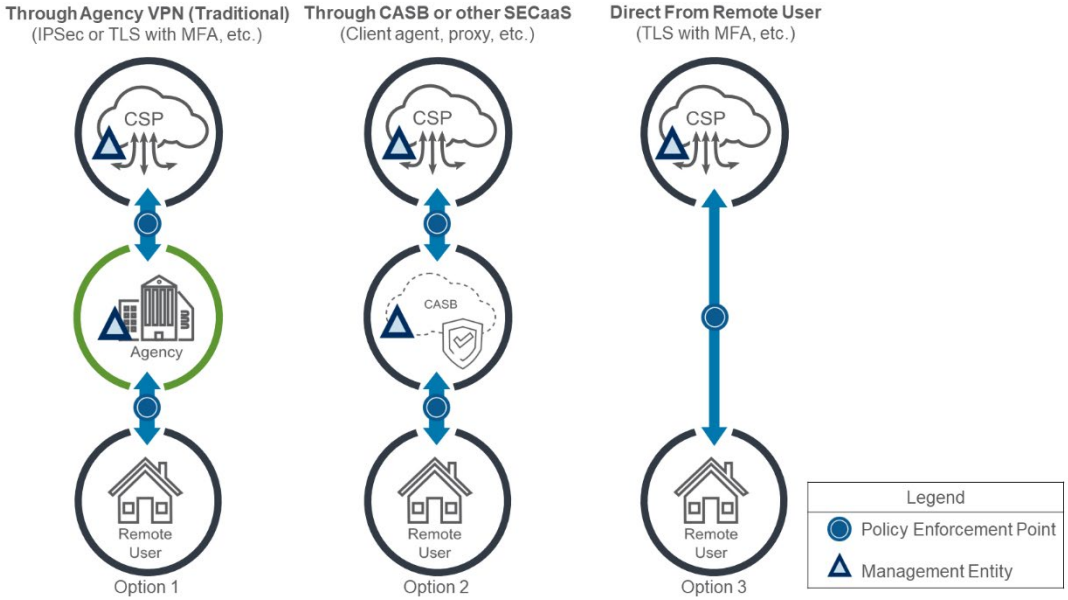


Figure 6: Security Pattern 2: Remote User to Cloud Service Providers

The **first option** (left) aligns with traditional mechanisms for accessing CSP resources. Employing either option 1 or 2 from Security Pattern 1, the remote user establishes a protected connection (e.g., VPN or VDI) to the agency campus and accesses the resources on agency-sanctioned CSPs through that channel. This option facilitates policy enforcement parity for remote users through the use of the same protections and policy enforcement placement as Security Pattern 1.

The **second option** (left) permits connectivity from remote users to agency-sanctioned CSP resources through a CASB or other SECaaS provider. Policy enforcement can be performed at the CASB, the CSP, and, if possible, the remote user's device. Policy enforcement parity between remote users and on-premises agency users can be simplified when the entities use the same CASB or SECaaS provider. Remote users establish a protected connection to the CASB. Various methods can be used to direct remote user traffic to the CASB, including client agents, proxy settings, and DNS means. The CASB trust zone is labeled with a medium trust level in this option, though agencies may determine and label trust zones according to the trust levels that best describe their environment.

The **third option** (left) permits connectivity from remote users directly to agency-sanctioned CSP resources via protected connections (e.g., TLS and MFA). Policy enforcement placement and protections are applied at the CSP and, if possible, on the remote user's device. Policy enforcement parity between remote users and on-premises agency users can be simplified when protections are handled at the CSP and applied consistently no matter the location of the agency entity accessing the resource.

6.3 SECURITY PATTERN 3: REMOTE USER TO THE WEB

Figure 7 illustrates the scenario when the remote user accesses untrusted web-based resources on the web. There are three options for this connectivity. Connections in this security pattern are the riskiest because of the connection from an agency entity to a low trust zone. This will require the greatest amount of rigor to be applied to the capabilities.

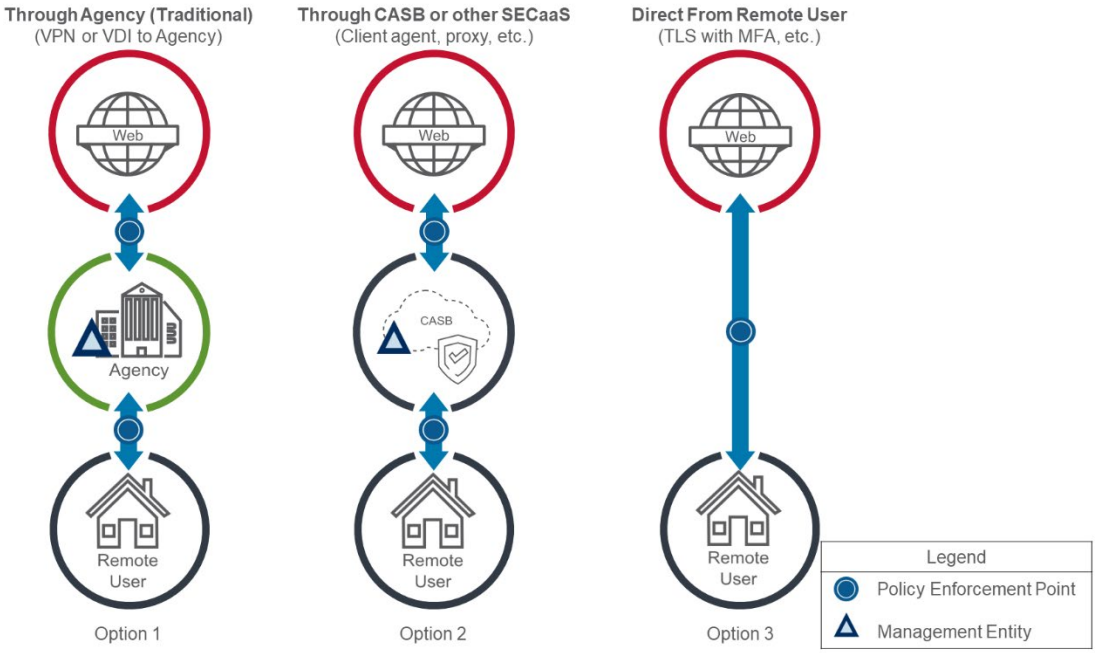


Figure 7: Security Pattern 3: Remote User to the Web

The **first option** (left) aligns with traditional mechanisms for accessing the web. The remote user establishes a protected connection (e.g., VPN or VDI) to the agency campus and accesses the web through that channel. This option facilitates policy enforcement parity for remote users through the use of the same protections and policy enforcement placement as Security Pattern 1.

The **second option** (left) permits connectivity from remote users to the web through a CASB or other SECaaS provider. Policy enforcement can be performed at the CASB and, if possible, the remote user's device. Policy enforcement parity between the remote users and on-premises agency users can be simplified when the entities use the same CASB or SECaaS provider. Remote users establish a protected connection to the CASB. Various methods can be used to direct remote user traffic to the CASB, including client agents, proxy settings, and DNS means. The CASB trust zone is labeled with a medium trust level in this option, though agencies may determine and label trust zones according to the trust levels that best describe their environment.

The **third option** (left) permits connectivity from remote users directly to resources on the web. Policy enforcement placement and protections can only be applied at the remote user's device. This will limit policy enforcement parity due to limitations in the types of protections that can be deployed to these devices. Given these constraints and the effect they have on the trust an agency may place in the remote user's device in the other security patterns, agencies may need to apply additional protections in connected environments to manage the risks associated with the use of this option.

7. APPICABLE SECURITY CAPABILITIES

The Security Capabilities Catalog [8] contains a table of universal and PEP security capabilities that apply across use cases, but not all apply to every use case. Each will contain a set of relevant security capabilities, based on agency pilot implementations and best practices. Additional security capabilities may be employed by agencies to reflect agency requirements, risk tolerances, and other factors. The Remote User Use Case is one use case where some PEP security capabilities are not applicable. For traceability, the security capabilities not included in this use case are listed below by PEP capability group.

- Email: Authenticated Received Chain
- Intrusion Detection: Deception Platforms
- Enterprise: Costs Monitoring
- Services: All capabilities in this functional group are not applicable.
- Identity: Service Identity

[8] This use case references *Trusted Internet Connections 3.0 Security Capabilities Catalog,* v2.0, dated October 2021.

7.1 UNIVERSAL SECURITY CAPABILITIES

Universal security capabilities are enterprise-level capabilities that outline guiding principles for TIC use cases and apply across use cases. Agencies have the discretion to determine the level of rigor necessary for applying universal security capabilities based on federal guidelines and their risk tolerance.

Table 3 provides a list of the universal security capabilities that apply to the Remote User Use Case and implementation guidance for agencies to consider. Most agencies will have an existing enterprise solution for the universal security capabilities; as agencies deploy the Remote User Use Case, the guidance below can be integrated into their existing solutions. While universal security capabilities are broadly applicable, the circumstances and threats associated with remote users require agencies to consider the security challenges that may need to be addressed.

Table 3: Universal Security Capabilities

Capability	Description	Use Case Guidance
Backup and Recovery	Backup and recovery entails keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures, or corruption.	Agencies should ensure that relevant configuration and data from remote user devices are being backed up. Since remote user devices may be in unprotected locations, these backups should, if possible, be to a more secure location (e.g., the agency campus, an externally hosted backup service, etc.). If an agency is unable to back up a given user device, there should be policies in place to minimize the consequences of failure or loss of the device. These policies may include limiting what work is conducted on these devices, specifying when work conducted on these devices must be synchronized with or sent to the agency, or limiting the amount or types of data stored solely on user devices.
Central Log Management with Analysis	Central log management with analysis is the collection, storage, and analysis of telemetry, where the collection and storage are designed to facilitate data fusion and where the security analysis aids in discovery and response to malicious activity.	Agencies should, when possible, collect device logs from remote user devices. Agencies should also collect logs from the services, including security services, that remote users interact with to ensure visibility into the remote user device actions, even

Capability	Description	Use Case Guidance
		if the agency cannot collect relevant telemetry from the remote user devices. Agencies should consult M-21-31 on log management.[9] Given the increased chance for data exfiltration or loss, agencies should track data sent to and received from remote user devices. These logs should, when possible, be integrated with the agency's central log management solution and shared with NCPS[10], as requested by CISA for situational awareness.
Configuration Management	Configuration management is the implementation of a formal plan for documenting and managing changes to the environment, and monitoring for deviations, preferably automated.	Agencies should, when possible, employ device management solutions that allow the automatic deployment of policies to agency remote devices. For devices that agencies cannot apply policies to, agencies may provide guidance to their users about applying policies to their devices. Agencies should not assume correct application but should provide compensating controls elsewhere. When possible, agencies should verify device configuration compliance when authorizing access to agency networks, services, and data. This compliance should be verified in an ongoing manner while a device maintains access to agency networks or services.
Incident Response Plan and Incident Handling	Incident response planning and incident handling is the documentation and implementation of a set of instructions, procedures, or technical capabilities to sense and detect, respond to, limit consequences of malicious	Agency incident response and handling should account for remote user devices. Agencies should track remote users' access to agency services and data, especially for actions inconsistent with typical remote usage. Agencies should

[9] "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," Office of Management and Budget M-21-31 (2021). 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.
[10] "National Cybersecurity Protection System (NCPS)," https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

Capability	Description	Use Case Guidance
	cyberattacks, and restore the integrity of the network and associated systems.	monitor CSP and other external services for misuse or breach and adapt response plans and activities accordingly.[11]
Inventory	Inventory entails developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access, and unauthorized and unmanaged devices are found and restricted from gaining access.	Agency-owned remote user devices should be included in agency device inventory solutions, including type of device, device user, deployed applications, and policies, patching status of the device and application, and device compliance. Agencies should leverage the CDM capabilities.[12]
Least Privilege	Least privilege is a design principle whereby each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	Agency users' access to agency services and data should consider the security of the device used to access the service or data, enabling higher levels of access to users with more secure devices.
Secure Administration	Secure administration entails securely performing administrative tasks, using secure protocols.	If agencies permit administration of services by remote users, they should employ MFA and account for device security and compliance before authorizing administrative access. Agencies should consider limiting administrative access using methods like VPNs, jump servers, and bastion hosts. Agencies should track and analyze administrative logins and activities, especially when inconsistent with normal usage, and should have procedures for quickly revoking administrative access. Agencies should develop policies and procedures to allow remote desktop support services, device patch management across remote connections, and local user privilege level modifications as needed.

[11] CISA resources on incident management can be found at https://www.cisa.gov/cyber-incident-response.
[12] "Continuous Diagnostics and Mitigation (CDM)," https://www.cisa.gov/cdm.

Capability	Description	Use Case Guidance
Strong Authentication	Strong authentication verifies the identity of users, devices, or other entities through rigorous means (e.g., multi-factor authentication) before granting access.	Agencies should ensure users are authenticated to all agency servers using MFA[13], in accordance with OMB M-19-17.[14]. When considering MFA solutions that allow for short message service (SMS), agencies should account for the possibility of subscriber identity module (SIM)-swapping attacks. If MFA is unsupported by a service, strong password policies should be in place with the service, ensuring that no passwords are reused. Consult NIST 800-63 *Digital Identity Guidelines*.[15] for additional guidance on authentication and when to require reauthentication. Consider risk-based authentication to determine when additional verification is required before or during access to networks, hosts, services, or resources. Risk-based authentication may consider characteristics such as device security posture, IP address, geolocation, and time of access or the risk potential of the connection. Remote user connections often represent a greater risk than traditional network architectures, placing a greater reliance on secure authentication mechanisms for validation.[16]

[13] "CISA Phishing Resistant Multifactor Authentication," www.cisa.gov/mfa.
[14] "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," Office of Management and Budget (2019). https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.
[15] "Digital Identity Guidelines," National Institute of Standards and Technology. https://pages.nist.gov/800-63-3/
[16] See the Implementing Strong Authentication Capacity Enhancement Guide for more information: https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Implementing_Strong_Authentication_508_1.pdf.

Capability	Description	Use Case Guidance
Time Synchronization	Time synchronization is the coordination of system (e.g., servers, workstations, network devices) clocks to minimize the difference between system clock times and enable accurate comparison of timestamps between systems.	Agency user devices should be synchronized. However, given the difficulties in ensuring clock synchronization across all devices that agency users may use, agencies should obtain telemetry about agency user activity from the services, including security services, where the agency can more readily ensure timestamp accuracy.
Vulnerability Management	Vulnerability management is the practice of proactively working to discover vulnerabilities by including the use of both active and passive means of discovery and by taking action to mitigate discovered vulnerabilities.	Agencies should work with the users to help ensure the security of their devices and, if possible, their networks. Agency user devices should have appropriate protections in place, including firewalls and anti-malware, whether applied automatically by agency device policies or manually by the agency user. Agencies should account for changes in user location in their overall vulnerability assessment procedures. These procedures should include assessments of remote user devices, accounting for the new access points to the agency and to CSP environments, and assessments of agency vulnerability to data loss and theft.[17]

[17] More information on vulnerability management can be found at https://www.cisa.gov/cdm.

Capability	Description	Use Case Guidance
Patch Management	Patch management is the identification, acquisition, installation, and verification of patches for products and systems.	Agency remote user devices may be used or connected to the agency network intermittently, with the potential for delays in applying patches and resultant windows of vulnerability. Critical patches (which fix known security vulnerabilities) should be identified per agency risk tolerances. To ensure timely patching, critical patch advisories should be communicated to remote users, particularly to encourage patching of unmanaged devices. Agencies should track which devices have been patched and should assume that remote devices have not been patched until confirmed otherwise. Based upon agency risk tolerances, unpatched devices may merit follow up with the remote user and access restrictions on those devices until patched, particularly if active exploits are known.[18]
Auditing and Accounting	Auditing and accounting includes capturing business records (e.g., logs and other telemetry), making them available for auditing and accounting as required, and designing an auditing system that considers insider threat (e.g., separation of duties violation tracking) such that insider abuse or misuse can be detected.	Cloud service licensing, activity, and billing may require adaptation to existing tracking mechanisms. Agencies should ensure compatibility and interoperability to minimize visibility gaps.
Resilience	Resilience entails ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.	Agencies should proactively work to ensure agency services have the capability to scale as necessary to handle remote work by agency users.

[18] See the CISA Remote Patch and Vulnerability Management Capacity Enhancement Guide for more information: https://www.cisa.gov/publication/capacity-enhancement-guides-federal-agencies.

Capability	Description	Use Case Guidance
Enterprise Threat Intelligence	Enterprise threat intelligence is the usage of threat intelligence from private or government sources to implement mitigations for the identified risks.	Agencies should seek out and adopt any new threat intelligence feeds[19] which align with new services or delivery mechanisms deployed, and with threats to and from remote users and devices.
Situational Awareness	Situational awareness is maintaining effective current and historical awareness across all components.	Agencies should maintain awareness of the remote users and their devices, including threats that may be specific to those users or locations. Agencies may need to obtain this awareness from the agency services. Agencies should seek integration of CSP telemetry into centralized situational awareness tools.
Dynamic Threat Discovery	Dynamic threat discovery is the practice of using dynamic approaches (e.g., heuristics, baselining, etc.) to discover new malicious activity.	Agencies should track agency users' use of agency services or data, including device information, if possible, to look for changes or discrepancies. This is especially important when agency users are working remotely.
Policy Enforcement Parity	Policy enforcement parity entails consistently applying security protections and other policies, independent of the communication mechanism, forwarding path, or endpoints used.	Agencies should ensure integrated desktop, mobile, and remote policies align. Care must be taken to ensure any new remote user endpoint protections align with established agency risk tolerances.
Effective Use of Shared Services	Effective use of shared services means that shared services are employed, where applicable, and individually tailored and measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external and internal to the service provider.	Shared services can improve remote user resource usability, increase service availability and resilience, and enhance user experience. Agencies should carefully consider security capabilities when selecting shared service providers. Agencies should consider regional delivery opportunities so that shared services

[19] To learn more about different threat intelligence models, see https://www.cisa.gov/publication/service-models-cyber-threat-intelligence-white-paper. Agencies can also participate in CISA's cyber threat indicator sharing program, called Automated Indictor Sharing: https://www.cisa.gov/ais.

Capability	Description	Use Case Guidance
		can be deployed closer to remote user locations.
Integrated Desktop, Mobile, and Remote Policies	Integrated desktop, mobile, and remote policies define and enforce policies that apply to a given agency entity independent of its location.	Agencies should employ methods to define user policies in line with each agency's abilities to enforce policies. If an agency policy allows a user to use a device that the agency cannot enforce policies on, then the policy may need to be enforced, if possible, at the service or data level, or the user may need to be restricted from accessing the service or data. Agencies should ensure security parity across policies for devices to ensure consistent protection and to minimize user workarounds that could bypass desired security.
User Awareness and Training	User awareness and training entails that all users are informed of their roles and responsibilities and appropriate cybersecurity education is provisioned to enable users to perform their duties in a secure manner.	Agency users should understand their responsibilities in protecting agency devices and data that they have taken off-site. Agencies should ensure that users understand the security concerns for devices and networks that are not managed by the agency, and potential ways to mitigate some of these concerns. Agencies may need to augment their phishing training to account for the increased potential for phishing while off-site. If the agency does not automatically backup data from remote user devices, agency users must understand how to protect against data loss while working remotely.
Supply Chain Risk Management	Supply chain risk management involves implementing a systematic process for managing risk exposures, threats, and vulnerabilities throughout the cyber supply chain. It also involves developing risk-response strategies for the risks presented by the supplier, the	When possible, devices used for processing agency data should be procured by agencies through trusted suppliers. By operating outside traditional agency campuses, it may be more difficult for remote agency users to obtain new or replacement products from trusted suppliers.

Capability	Description	Use Case Guidance
	supplied products and services, or the supply chain.	Agencies could work with their trusted supplier to facilitate use by remote users. Agencies could also work with remote users to ensure they have access to sufficient backup products or appropriate workarounds to enable business continuity while remote. Agencies may also consider mechanisms to allow remote users to use products obtained from other suppliers if appropriate protections are in place to mitigate the potential for compromise.
Resource Lifecyle Management	Resource lifecycle management is the end-to-end process of managing resources from development to operation to retirement, such that resources are provisioned and decommissioned in conjunction with the applications they support.	Agencies should track all agency-owned computing hardware, including remote hardware, in an asset management database. Damaged or end-of-life hardware should be returned to agencies for decommission and not disposed by a remote user.
Security Test and Exercise	Security tests (e.g., penetration testing or red teaming) verify the extent to which a system resists active attempts to compromise its security. Security exercises are simulations of emergencies that validate and identify gaps in plans and procedures.	Agencies should understand the threats and vulnerabilities of their remote user devices to ensure comprehensive security testing. Agencies should perform regular security test and exercise routines that include remote user devices. These exercises should simulate situations where remote user devices are used as the source of attacks against agency resources as well as exercises where remote user devices are being attacked. Where security tests are performed against the devices of remote users, agencies should consider methods that minimize the potential disruption for the remote user (e.g., performing tests outside of business hours).

Capability	Description	Use Case Guidance
Continuous Monitoring Reporting	Continuous monitoring reporting entails the maintenance of ongoing awareness of informational security, vulnerabilities, and threats to support organizational risk management decisions.	Agencies should keep up to date on the latest vulnerabilities and threats to make more informed decisions on security risk mitigations for remote users. Agencies should understand the timeliness of telemetry received from remote user devices as well as any potential limits in visibility provided to ensure an accurate understanding of the risks to and potential vulnerabilities for remote users.
Governance and Policy Auditing	Governance and policy auditing entails validating the proper definition, application, and enforcement of agency rules and policies.	Agencies should regularly review applicable rules and policies to ensure their relevance, compliance, and enforcement for remote users, as the potential changes in control and visibility may require tailoring. Agencies might consider encouraging users to connect to agency resources, when possible, to increase visibility and ensure device compliance.

7.2 POLICY ENFORCEMENT POINT SECURITY CAPABILITIES

PEP security capabilities are focused on the network level and inform technical implementation for a given use case, such as remote user communication with agency-sanctioned CSPs. Agencies have the discretion to determine the applicability and level of rigor necessary for applying PEP security capabilities based on the resources accessed by remote users, the policy enforcement options available, federal guidelines, and risk tolerance. From the Security Capabilities Catalog, the PEP security capability groups applicable to the Remote User Use Case correspond to the following security functions:

- Files,
- Email,
- Web,
- Networking,
- Resiliency,
- DNS,
- Intrusion Detection,
- Enterprise,
- Unified Communications and Collaboration (UCC),
- Data Protection, and
- Identity

Agencies may determine the applicability and rigor of the security capabilities based on federal guidelines, mission needs, available policy enforcement options, and risk tolerance.

Security capabilities that are not applicable to this use case are listed at the beginning of Section 7. The PEP security capability listing is not exhaustive. Additional security capabilities may be deployed by agencies to reflect their risk tolerances, early adoption of security capabilities, the maturity level of existing cyber programs, etc.

7.2.1 Files PEP Security Capabilities

With agency users operating outside traditional agency boundaries, agency file protections may need to be augmented to ensure commensurate file protections are provided for remote users. File protections may need to be tuned to account for the diversity of devices, locations of remote users, differences in roles and workflows employed while working remotely, and the threats to remote users.

Agencies should, when possible, apply file protections to any files transmitted to remote user devices, independent of their source (e.g., via email, via web browsing, via software patching services, etc.). These protections could be applied to files prior to their transmission to the remote user device (e.g., on the email server or at the web client proxy) in addition to the remote user devices themselves to help protect against files obtained through alternate means. Additionally, agencies should apply file protections to files received by the agency from remote user devices.

Table 4 lists the applicable Files PEP Security Capabilities for the Remote User Use Case.

Table 4: Files PEP Security Capabilities

Capability	Description	Use Case Guidance
Anti-malware	Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.	Agencies should, when possible, apply anti-malware protections on files before they are transmitted to the remote user devices. To protect remote user devices against files obtained through alternate means, agencies should, when possible, have anti-malware protections deployed to remote user devices. If remote users can employ a variety of device types, agencies should verify the breadth of coverage of their anti-malware protections and augment if needed to ensure sufficient coverage.

Capability	Description	Use Case Guidance
Content Disarm and Reconstruction	Content disarm and reconstruction technology detects the presence of unapproved active content and facilitates its removal.	If remote users can employ a variety of device types, agencies may consider using content disarm and reconstruction to remove active content from files before delivery to the remote user to decrease the attack surface across all device types. As content disarm and reconstruction technologies can interfere with users' ability to obtain needed documents, agencies should consider ways for their users to access the original file, or methods for remote users to receive unmodified files from trusted sources.
Detonation Chamber	Detonation chambers facilitate the detection of malicious code using protected and isolated execution environments to analyze the files.	Detonation chambers are difficult protections to deploy to remote user devices. Knowing this, agencies should consider detonation chamber technologies as part of their check for malicious files prior to the file being sent to remote users. Agencies should consider technologies that perform file detonation across the types of devices and environments that remote users may use.
Data Loss Prevention	Data loss prevention (DLP) technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Agency DLP solutions should account for exfiltration of agency data through remote user devices, with increased security rigor on file types, content, and volume of information permitted on remote user devices. Agency DLP may need to account for methods for accessing data, especially data stored in external environments, that bypass traditional infrastructure. Remote user technical enforcement may need to be supplemented with additional administrative controls that address data handling and use when accessing services remotely.

7.2.2 Email PEP Security Capabilities

Environments with remote users can present significant challenges associated with mitigating email-based threats (e.g., phishing). This challenge is amplified since agencies have limited visibility and control over remote user devices, increasing reliance on the email service as a means for meaningful policy enforcement. When remote users are accessing email from remote locations, the protections available to them when using an agency-managed endpoint in an on-premises environment may no longer be available at the same enforcement and performance levels.

The importance of email services for business operations may also increase, as remote users may not be able to leverage alternative communication means to the same degree as when on-premises. This can lead to the email system becoming a more attractive target for adversaries, as the breadth and depth of agency data hosted within the email system increases. Table 5 lists the applicable Email PEP Security Capabilities for the Remote User Use Case.

Table 5: Email PEP Security Capabilities

Capability	Description	Use Case Guidance
Anti-phishing Protections	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	Agencies should ensure that their anti-phishing protections are tuned to the threats for remote users. Beyond email protection solutions, agencies should work with their users to ensure they understand the phishing threat since attackers may use alternative vectors (e.g., SMS, telephone, etc.) in their phishing attempts.[20]
Anti-spam Protections	Anti-spam protections detect and quarantine instances of spam.	No specific guidance.
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Agency DLP solutions should account for exfiltration of agency email and data through remote user devices, with increased security rigor on file types, content, and volume of information permitted on remote user devices. Remote user technical enforcement may need to be supplemented with additional administrative controls that address data handling and use when accessing services remotely.
Domain Signature	Domain signature verification protections authenticate incoming	Agencies may consider strengthening their DMARC protections (e.g.,

[20] See the CISA Capacity Enhancement Guide on Counter Phishing Recommendations for Federal Agencies for more information: https://www.cisa.gov/publication/capacity-enhancement-guides-federal-agencies.

Capability	Description	Use Case Guidance
Verification for Incoming Email	email according to the Domain-based Message Authentication Reporting and Conformance (DMARC) email authentication protocol defined in Request for Comments (RFC) 7489. [21]	quarantining emails that fail to pass security checks) to decrease the opportunities for malicious emails to be received by the remote users.
Domain Signatures for Outgoing Email	Domain signature protections facilitate the authentication of outgoing emails by signing the emails and ensuring that external parties may validate the email signatures according to the DMARC email authentication protocol that is defined in RFC 7489.	Agencies should consider strengthening DMARC protections for outgoing emails to decrease attackers' ability to impersonate the agency (e.g., updating sender policy framework (SPF) records to "deny-all" for domains and subdomains which do not send email). These protections can be important even when other agency email protections are in place as attackers may target the personal email accounts of remote users.
Encryption for Email Transmission	Email services are configured to use encrypted connections, when possible, for communications between clients and other email servers.	Agencies should ensure that only encrypted methods of email transmission are available for use to ensure the confidentiality and integrity of email, even when transmitted over potentially untrusted networks.
Malicious Link Protections	Malicious link protections detect malicious links in emails and prevent users from accessing them.	Agencies should consider applying malicious link protections to the remote user's email upon receipt to prevent the device from receiving the malicious link in the first place.
Link Click-through Protections	Link click-through protections ensure that when a link from an email is clicked, the requester is directed to a protection that verifies the security of the link destination before permitting access.	While malicious link protections can protect against known bad links, the protections can miss certain malicious links (e.g., if a nominally benign link becomes malicious). As remote users may not be accessing emailed links through agency boundary web protections, there may be no opportunity for protecting against these types of attacks. Agencies should consider link click-through protections which force the remote user's link access to traverse

[21] "Domain-based Message Authentication, Reporting, and Conformance Request for Comments: 7489," Internet Engineering Task Force (2015). https://tools.ietf.org/html/rfc7489.

Capability	Description	Use Case Guidance
		agency protections, even in situations where the remote user device is not using agency protections for its typical web access.
EINSTEIN 3 Accelerated Email Protections	EINSTEIN 3 Accelerated (E3A) is an intrusion prevention capability offered by NCPS, provided by CISA, that includes an email filtering security service.	No specific guidance.
Sender Denylisting	Sender denylisting protections prevent the reception of email from denylisted senders, domains, or email servers.	No specific guidance.
Post-Delivery Protections	Post-delivery protections apply updated email protections to already delivered emails, enabling quarantining and mitigation for emails in mailboxes.	Post-delivery protections can be more difficult to provide to remote users, as they are not always connected to agency networks and will receive updated policies later than local users. Agencies should consider requiring remote assets to connect to the network regularly to mitigate this.
Malicious File Protections	Malicious file protections detect malicious attachment files in emails and prevent users from accessing them.	As remote user devices may have more limited resources or protections available, agencies should consider enabling malicious file protections for email attachments prior to the transmission to a remote user device. Malicious file protections should allow for detection both on receipt by the mail server as well as retroactively when updated determinations can be made. Agencies should consider malicious file protections that apply both static and dynamic analysis techniques (e.g., sandboxes).
Adaptive Email Protections	Adaptive email protections involve employing risk-based analysis in the application and enforcement of email protections.	Agencies should consider adaptive protections that can account for the additional context of remote users, including factors such as user location, device compliance, or user behavior.
Email Labeling	Email labeling is the process of automatically tagging incoming or outgoing email to manage risk.	No specific guidance.

Capability	Description	Use Case Guidance
User Tipping	User tipping capabilities enable users to report emails, attachments, or links they suspect to be phishing attempts, spam, or otherwise malicious.	Agencies should ensure that remote users can effectively employ user tipping capabilities to report suspected malicious activity. Additionally, as attackers may target the personal email accounts of remote users, agencies may consider methods to enable users to report these attempts by malicious actors.
Content Filtering	Content filtering protections detect the presence of unapproved content and facilitate its removal or denial of access.	Agencies should enable content filtering capabilities to prevent potential spread of unapproved content. Agencies might tune their content filtering to account for various risks associated with remote users by considering the use of information such as remote device type and device location. Content filtering should consider applying content filtering protections to all content going to and from the remote user.
User Digital Signatures for Outgoing Email	User digital signature protections enable users to digitally sign emails, allowing external parties to authenticate the email's sender and its contents.	When implementing user digital signatures, agencies may consider digital signature solutions where the email signing and user certificates are deployed to the email service. Alternatively, agencies may deploy user digital signature solutions to users' devices potentially facilitating their use. When deploying to end user devices, agencies should consider the protections and policies to mitigate opportunities to compromise the user signing certificates, whether through software or physical compromise. The types of protections and policies that can be applied may be affected by the level of visibility and control the agencies maintain over the end user devices. To account for the loss or compromise of user certificates, agencies should consider mechanisms to revoke lost or compromised user certificates and to generate and distribute new user certificates.

Capability	Description	Use Case Guidance
Encryption for Outgoing Email	Email encryption protections allow for the encryption of outgoing emails, which limits the visibility of their contents to the intended recipients.	To facilitate the sharing of agency data with remote users via email, agencies may consider protections that enable end-to-end encryption of email content and attachments. Since remote users may access email from different locations and devices, the methods for enabling end-to-end encryption should allow for remote users to access their encrypted emails from these locations and devices, in line with agency risk tolerance. When deploying to end user devices, agencies should consider the protections and policies to mitigate opportunities to compromise the encrypted emails, whether through software or physical compromise. Agencies should understand any effects this encryption might have on enterprise visibility or the types of protections that can be applied.
Mail Content Query	Mail content query enables search and discovery for email across agency mailboxes.	Remote user devices often keep local copies of their emails to improve user experience while working remotely. Agencies should understand and account for any potential differences between the user mailboxes on the email services and user mailboxes on their devices (e.g., when a user is working without access to the email service).
Email Domain Reputation Protection	Email domain reputation protection entails monitoring an email domain's reputation and employing policies to help protect the email domain's reputation.	No specific guidance.

7.2.3 Web PEP Security Capabilities

Agencies should, if possible, apply web capabilities commensurate to those available from the agency campus to all data flows from the remote users containing web traffic. Beyond accessing web resources, these data flows could also include access to CSPs, whether agency-sanctioned or not. Remote user traffic may no longer traverse traditional policy enforcement positions, requiring an increased reliance upon server and service-side inspection and policy enforcement.

Remote users may have specialized roles that permit a more granular approach to the enforcement of web protections than bulk on-premises solutions. When accessing agency-sanctioned web-based

Capability	Description	Use Case Guidance

services, agencies may need to bypass certain protection positions for functional, performance, or other reasons. In these scenarios, agencies should ensure that compensating protections are in place to sustain policy enforcement parity. In addition, the protections provided to a remote user may need to be augmented for the specific threats or environment of the remote user. Table 6 lists the applicable Web PEP Security Capabilities for the Remote User Use Case.

Table 6: Web PEP Security Capabilities

Capability	Description	Use Case Guidance
Break and Inspect	Break and Inspect systems, or encryption proxies, terminate encrypted traffic, logging or performing policy enforcement against the plaintext, and re-encrypting the traffic, if applicable, before transmitting to the final destination.	Agencies should consider the protections afforded to and lifetimes for certificates used as part of Break-and-Inspect certificates to decrease the chance of compromise and mitigate the effects to remote users of certificate compromise. Agencies should consider device loss or theft when determining certificate or keying material to host on remote user endpoints and the scope of changes required if these materials become compromised.
Active Content Mitigation	Active content mitigation protections detect the presence of unapproved active content and facilitate its removal.	Agencies may need to tune their active content mitigation to account for differences in the threats to and web usage of remote users, including incidental personal use. Agencies may also need to augment these protections as remote user devices may only have intermittent access to receive updates.
Certificate Denylisting	Certificate denylisting protections prevent communication with entities that use a set of known bad certificates.	Agencies may need to tune their certificate denylisting to account for differences in the threats to and web usage of remote users, including incidental personal use. Agencies may also need to augment these protections as remote user devices may only have intermittent access to receive updates.

Capability	Description	Use Case Guidance
Content Filtering	Content filtering protections detect the presence of unapproved content and facilitate its removal or denial of access.	Agencies may need to tune their content filtering to account for differences in the threats to and web usage of remote users, including incidental personal use. Agencies may also need to augment these protections as remote user devices may only have intermittent access to receive updates.
Authenticated Proxy	Authenticated proxies require entities to authenticate with the proxy before making use of it, enabling user, group, and location-aware security controls.	Agencies should consider the use of authenticated proxies for remote users to allow for eligibility enforcement and more centralized policy enforcement positioning and reducing reliance on remote user endpoints for policy enforcement.
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Agency DLP solutions should account for file exfiltration through remote user devices, with increased security rigor on file types, content, and volume of information permitted on remote user devices. Agency DLP may need to account for methods of accessing data, especially data stored in external environments, that bypass traditional infrastructure. Remote user technical enforcement may need to be supplemented with additional administrative controls addressing data handling and use when accessing services remotely.
Domain Resolution Filtering	Domain resolution filtering prevents entities from using unauthorized DNS resolution services over the DNS-over-Hypertext Transfer Protocol Secure (HTTPS) domain resolution protocol.	Agencies should consider DNS-over-HTTPS filtering in the overall context of ensuring secure DNS for their remote users who may be connected to untrusted networks. Agencies should ensure visibility is not lost, even if remote users bring devices back onto the traditional on-premises networks.

Capability	Description	Use Case Guidance
Protocol Compliance Enforcement	Protocol compliance enforcement technologies ensure that traffic complies with protocol definitions, like those documented by the Internet Engineering Task Force (IETF).[22]	Agencies may consider enabling more stringent policy enforcement, as the variety of business services increasingly employs web services. Use of proxy services can simplify protocol compliance enforcement at the proxy component within agency visibility and control.
Domain Category Filtering	Domain category filtering technologies allow for classes of domains (e.g., banking, medical) to receive a different set of security protections.	Agencies may need to tune their domain category filtering to account for differences in the threats to and web usage of remote users, including incidental personal use. Agencies may also need to augment these protections as remote user devices may only have intermittent access to receive updates.
Domain Reputation Filtering	Domain reputation filtering protections are a form of domain denylisting based on a domain's reputation, as defined by either the agency or an external entity.	Agencies may need to tune their domain reputation filtering to account for differences in the threats to and web usage of remote users, including incidental personal use. Agencies may also need to augment these protections as remote user devices may only have intermittent access to receive updates.
Bandwidth Control	Bandwidth control technologies allow for limiting the amount of bandwidth used by different classes of domains.	Agencies may need to update and enforce rules of behavior or other policies to ensure remote users' incidental personal web use does not adversely impact business functionality on shared resources.

[22] "RFCs," Internet Engineering Task Force (2021). https://www.ietf.org/standards/rfcs/.

Capability	Description	Use Case Guidance
Malicious Content Filtering	Malicious content filtering protections detect the presence of malicious content and facilitate its removal.	Agencies may need to tune their malicious content filtering to account for differences in the threats to and web usage of remote users, including incidental personal use. Agencies may also need to augment these protections as remote user devices may only have intermittent access to receive updates.[23]
Access Control	Access control technologies allow an agency to define policies limiting what actions may be performed by connected users and entities.	Agencies should apply least function and deny-all-permit-by-exception principles when granting remote users' access to web services.

7.2.4 Networking PEP Security Capabilities

With remote users accessing agency services from outside the traditional agency networks, agencies have much less control over the devices used to access services and data. It may be prudent for agencies to assume remote user devices end up compromised. While agencies should consider health and policy compliance of the remote user's device as part of authorizing access to agency services and data, agencies should also strongly limit users' access to only the services or data that they require to help mitigate the risks of compromise. These protections may need to be applied on agency networks as well as on any cloud environments that remote users access. Table 7 lists the applicable Networking PEP Security Capabilities for the Remote User Use Case.

[23] See the CISA Capacity Enhancement Guide on Securing Web Browsers and Defending Against Malvertising for Federal Agencies for more information: https://www.cisa.gov/publication/capacity-enhancement-guides-federal-agencies.

Table 7: Networking PEP Security Capabilities

Capability	Description	Use Case Guidance
Access Control	Access control protections prevent the ingest, egress, or transiting of unauthorized network traffic.	Agencies should consider device health checks and security posture as part of allowing access to agency networks. Additionally, agencies should consider requiring MFA to mitigate the effects of password compromise, device loss or theft, or device impersonation. Remote user devices should have firewalls and other network-level protections enabled to decrease their threat surface when used on untrusted networks.
Internet Address Denylisting	Internet address denylisting protections prevent the ingest or transiting of traffic received from, or destined, to a denylisted internet address.	As part of enabling access to agency services from remote locations, agencies should consider denying access from known or suspected malicious addresses.
Host Containment	Host containment protections enable a network to revoke or quarantine a host's access to the network.	Agencies should consider methods to revoke remote users' access to agency services or data since it may not be possible to revoke or quarantine the network access of remote user devices. Additionally, the inability to revoke a device's access to external networks may affect how agencies combat data exfiltration (e.g., remote wiping of agency data on the device, keeping agency data off the device in the first place, etc.).

Capability	Description	Use Case Guidance
Network Segmentation	Network segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks and decreasing the attack surface of the network.	Agencies should consider segmenting their networks, both on-premises and in cloud environments, under the assumption that remote user devices may become compromised. Segmenting agency networks limits remote users' access to only the services or data that they require can help mitigate these risks. This segmentation is especially important in VPN environments where the remote user device is bridged with an agency network.
Microsegmentation	Microsegmentation divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data.	With agency services employing increasingly complex workflows, especially when integrated with services deployed across cloud environments, agencies should consider a more fine-grained approach to network segmentation to more effectively limit remote users' access to only those services and data they require.

Capability	Description	Use Case Guidance
Resource Containment	Resource containment protections enable the removal or quarantine of a resource's access to other resources.	With remote users potentially accessing resources through different paths than on-premises users, agencies should understand all potential methods for accessing quarantined resources to ensure the effectiveness of controls. Agencies should have a similar understanding in order to apply resource containment controls to remote users, entities, or endpoints, limiting their access to agency resources even if brought back onto the traditional on-premises networks. Additionally, beyond manual application of resource containment, agencies should consider mechanisms to automatically contain user devices using risk-based determinations that consider characteristics such as device security posture, IP address, geolocation, etc.

7.2.5 Resiliency PEP Security Capabilities

Remote user devices often rely heavily on agency resources and authorized CSPs. As such, the availability of reliable, secure connections with sufficient bandwidth and low latency can be critical to remote user productivity. Additionally, the diversity of remote devices can vary dramatically, requiring agencies to prioritize breadth of endpoint support and alignment with open standards when deploying high availability services. Table 8 lists the applicable Resiliency PEP Security Capabilities for the Remote User Use Case.

Table 8: Resiliency PEP Security Capabilities

Capability	Description	Use Case Guidance
Distributed Denial of Service Protections	Distributed Denial of Service (DDoS) protections mitigate the effects of distributed denial of service attacks.	Remote users have a higher dependency on public-facing services, increasing the vulnerability of remote users to DDoS attacks.
Elastic Expansion	Elastic expansion enables agencies to dynamically expand the resources	The demand for remote user connectivity can be intermittent and vary significantly. Agencies should evaluate the maximum agency-

Capability	Description	Use Case Guidance
	available for services as conditions require.	required capacity (which can change with time and circumstances) and ensure that solutions are in place to elastically scale to cover those needs. The maximum agency-required capacity may be the maximum utilization without any degradation of service or may allow for an agency-determined acceptable level of service degradation.
Regional Delivery	Regional delivery technologies enable the deployment of agency services across geographically diverse locations.	Agencies should consider using regional service delivery to reduce latency for remote users, especially for services like VDI where higher latency can impact usability. Regional delivery can also reduce the impact of service failure to only locally connected users.

7.2.6 Domain Name System PEP Security Capabilities

To effectively operate outside the traditional agency networks, remote users need to be able to trust that agency domain names resolve and point to the appropriate resources. Agency users may be connecting to these agency services from a variety of network environments, some of which may not properly validate domain names and some of whom may have been compromised. To account for these, it may be prudent for remote users to manually specify DNS providers and, when possible, should use name resolution services with the same protections as endpoints on the agency campus.[24] Table 9 lists the applicable DNS PEP Security Capabilities for the Remote User Use Case.

Table 9: Domain Name System PEP Security Capabilities

Capability	Description	Use Case Guidance
Domain Name Sinkholing	Domain name sinkholing protections are a form of denylisting that protects clients from accessing malicious domains by responding to DNS queries for those domains.	Remote user devices should use DNS services that filter malicious traffic. These services may need to be configured on the device to ensure that appropriate DNS servers are used even on untrusted networks. If possible, the devices should use the same DNS services as the agency.

[24] Learn more about CISA's Domain Name Sinkholing service, called Protective DNS Resolver, at https://www.cisa.gov/cyber-qsmo-marketplace.

Capability	Description	Use Case Guidance
Domain Name Verification for Agency Clients	Domain name verification protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated according to Domain Name System Security Extensions (DNSSEC).	Remote user devices should use DNS services that validate DNS domains, including agency domains. These services may need to be configured on the device to ensure that appropriate DNS servers are used even on untrusted networks. If possible, the devices should use the same DNS services as the agency.
Domain Name Validation for Agency Domains	Domain name validation protections ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution to the domain names.	Agencies should host their domain names in DNS services that provide DNSSEC capabilities that allow remote users to validate the domains.
Domain Name Monitoring	Domain name monitoring allows agencies to discover the creation of or changes to agency domains.	Agencies should monitor for subdomains created under agency domains, or domains that mimic agency domains (e.g., domain squatting), as these could be used as part of phishing or other attacks against remote users.
CISA's Protective DNS Service	CISA's Protective DNS Service is a shared service offering that provides domain name sinkholing protections.	If Protective DNS protections need to be augmented or bypassed for remote user devices, agencies should work with CISA[25] to preserve commensurate protections and telemetry.

7.2.7 Intrusion Detection PEP Security Capabilities

An environment that allows users to access agency services and data from outside traditional agency networks has a different set of requirements than a traditional on-premises environment. With access to services coming from external parties, agencies retain much less control over remote user devices, especially in their ability to perform post-incident forensics. With less visibility and control in remote users' devices, it may be prudent to assume they may end up compromised and design the intrusion detection and prevention infrastructure accordingly (e.g., tailor access control to services or data based on the visibility and control over the remote users' devices, or look for anomalies in accessing data or use of services to detect malicious activity from the server side). Table 10 lists the applicable Intrusion Detection PEP Security Capabilities for the Remote User Use Case.

[25] OSMO@cisa.dhs.gov

Table 10: Intrusion Detection PEP Security Capabilities

Capability	Description	Use Case Guidance
Endpoint Detection and Response	Endpoint detection and response (EDR) tools combine endpoint and network event data to aid in the detection of malicious activity.	Agencies may need to augment their EDR solution as remote user devices may only intermittently provide telemetry or receive updated endpoint policies from agency EDR solutions.
Intrusion Detection and Prevention Systems	Intrusion detection systems (IDS) detect and report malicious activity. Intrusion prevention systems (IPS) attempt to stop the activity.	Agencies may need to tune their intrusion protection solutions to account for the differing malicious activity patterns and exploitation attempts that affect remote users. Agencies may need to augment their IPS solution to account for malicious attacks originating from remote user devices, including monitoring of the device itself as well as the user actions being initiated through the device.
Adaptive Access Control	Adaptive access control technologies factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.	Agencies should consider some unique attributes of remote users when making authorization decisions, including host security posture assessment, location, user credentials, timespan of sustained connection, presence of concurrent logins from diverse locations, changes in location since last login, etc. Additionally, agencies should consider requiring MFA to access data to mitigate the effects of password compromise, device loss or theft, or device impersonation.
Certificate Transparency Log Monitoring	Certificate transparency log monitoring allows agencies to discover when new certificates are issued for agency domains.	Agencies should monitor certificates being issued to detect domains that could be used as part of phishing or other attacks against remote users.
Network Detection and Response	Network detection and response involves the collection and analysis of network event data to aid in the detection and remediation of malicious activity.	When remote users can access agency services or networks, agencies may need to tune their network detection and response solutions to account for malicious activity behaviors associated with remote user access.

7.2.8 Enterprise PEP Security Capabilities

To effectively operate from outside traditional agency networks, remote users may need to remotely access agency services, data, and networks. The methods for doing so, including VPN and remote desktop access, can give a wealth of access to internal services. This access, coupled with the need to make services available to users connecting via the internet, requires extra care to ensure that these entry points are well-secured, including being up to date with security patches. These services should only be available using secure protocols (e.g., IP security and TLS) and should use MFA.

Agencies should consider mechanisms to revoke user or device access to agency services and data, to collect appropriate telemetry from remote user devices, and, if possible, to clear the remote endpoint of agency data on demand. Since remote user endpoints may be itinerant on agency infrastructure, care must be taken to ensure visibility is preserved in endpoint IT usage patterns. Consider endpoint caching of telemetry when between agency campus connected sessions, endpoint enforcement of connectivity to sanctioned services, and always-on protections to reduce visibility gaps. Table 11 lists the applicable Enterprise PEP Security Capabilities for the Remote User Use Case.

Table 11: Enterprise PEP Security Capabilities

Capability	Description	Use Case Guidance
Security Orchestration, Automation, and Response	Security Orchestration, Automation, and Response (SOAR) tools define, prioritize, and automate the response to security incidents.	Agencies may need to augment their SOAR solutions as remote user devices may only intermittently provide telemetry or be available for automated incident response.
Shadow Information Technology Detection	Shadow IT detection systems detect the presence of unauthorized software and systems in use by an agency.	Agencies should review collected telemetry for unsanctioned service use by remote users. Agencies may consider updating and retraining users on workflows and administrative controls for subscribing to new services for official business use.
Virtual Private Network	VPN solutions provide a secure communications mechanism between networks that may traverse across unprotected or public networks.	Agencies should ensure endpoint compliance checking and remediation takes place prior to establishing a full-featured VPN[26]. Only authorized services should be permitted to traverse the established VPN. Tunnel accepted security parameters should align with agency risk tolerances and be enforced.

[26] See the joint CISA and National Security Agency (NSA) Selecting and Hardening Remote Access VPN Solutions factsheet for more information: https://us-cert.cisa.gov/ncas/current-activity/2021/09/28/cisa-and-nsa-release-guidance-selecting-and-hardening-vpns.

Capability	Description	Use Case Guidance
Application Container	A virtualization approach in which applications are isolated to a known set of dependencies, access methods, and interfaces.	Agencies may utilize application containerization to limit access to agency services and data to specific applications running on remote user devices. If a remote user device is unmanaged, agencies may only be able to define policies at the application level. For agency-managed remote user devices, agencies may also be able to define policies at the device level.
Remote Desktop Access	Remote desktop access solutions provide a mechanism for connecting to and controlling a remote physical or virtual computer.	Remote desktop access may be provided as a direct service or in combination with a VPN. Remote desktop access should be made available using secure protocols and using strong authentication (e.g., MFA), especially if the remote desktop access is made available as a direct service. Agencies should prevent direct remote access to desktop instances by using protections like gateways or bastion hosts. For example, agencies should consider using a multi-tier architecture, allowing a front-end tier for user authentication and authorization, and thereby applying contextual security filters based on user or device location, operating system, and other factors. Agencies should consider preventing local file saving and peripheral use as well as strict enforcement of access application security settings.

7.2.9 Unified Communications and Collaboration PEP Security Capabilities

Remote users often need to participate in virtual meetings, which are frequently conducted using UCC tools. From a security and risk standpoint, the primary concerns are to make sure that only the desired content is shared with the intended people. To that end, UCC services that offer protections appropriate to the content to be shared should be selected. Protections offered can vary significantly between UCC vendors and even within a single vendor, where some of a vendor's offerings may be

certified to offer additional protections (e.g., FedRAMP or the Health Insurance Portability and Accountability Act (HIPAA)) while other versions lack those protections.[27]

Virtual meeting participants need to exercise caution and awareness of the content they are sharing to ensure that only authorized content is shared, including ensuring that microphones and/or cameras do not share unintended additional content or extraneous content when sharing screens. Participants also need to be aware that any content shared may be shared more widely than they intended; devices used by other attendees may use screen capture or otherwise record content. Care should be taken when sharing and receiving files, as well as when providing remote control to a computer, especially if left unattended. Table 12 lists the applicable UCC PEP Security Capabilities for the Remote User Use Case.

Table 12: Unified Communications and Collaboration PEP Security Capabilities

Capability	Description	Use Case Guidance
Identity Verification	Identity verification ensures that access to the virtual meeting is limited to appropriate individuals. Waiting room features, where the meeting host authorizes vetted individuals to join the meeting can also be utilized.	Agencies should consider using MFA as part of identity verification to mitigate the effects of password compromise, device loss or theft, or device impersonation. Remote users, especially those calling into meetings, may not be able to determine the identity of participants, increasing the importance of strong access control.
Encrypted Communications	Communication between virtual meeting participants and any data exchanged is encrypted at rest and in transit. Some UCC offerings support end-to-end encryption, where encryption is performed on the clients and can only be decrypted by the other authenticated participants and cannot be decrypted by the UCC vendor.	Agencies should ensure that only encrypted methods of communication are available for use by remote users, who may be using UCC tools over untrusted networks.
Connection Termination	Connection termination mechanisms ensure the meeting host can positively control participation through inactivity timeouts, on-demand prompts, unique access codes for each meeting, host participant eviction, and even meeting duration limits.	Agencies should have methods to revoke access for remote user devices to agency-managed UCC tools to account for the increased possibility of compromise or theft of remote user devices. The use of remote user devices in uncontrolled environments (e.g., hotel room) may increase the importance of inactivity timeouts.

[27] See CISA's Guidance for Securing Video Conferencing for more information: https://www.cisa.gov/publication/guidance-securing-video-conferencing.

Capability	Description	Use Case Guidance
Data Loss Prevention	Mechanisms should be implemented to control the sharing of information between UCC participants, intentional or incidental. This may be integrated into additional agency DLP technologies and can include keyword matching, attachment file type or existence prohibitions, attachment size limitations, or even audio/visual filters.	Agencies may augment their DLP solutions to account for remote users employing UCC tools without being connected to the traditional agency networks. Agency DLP solutions should account for file exfiltration through remote user devices, with increased security rigor on file types, content, and volume of information permitted on remote user devices.
Anti-phishing Protections	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	Agencies may need to tune their anti-phishing protection settings to address threats to remote users. When communications solutions enable end-to-end encryption, these protections may only be possible on the user endpoint device. When deploying endpoint protections, agencies should consider anti-phishing protections that can also apply to other methods of communication used by users (e.g., SMS). Beyond protection solutions, agencies should work with their users to ensure they understand the phishing threat since attackers may use alternative vectors (e.g., SMS, phone) in their phishing attempts.
Malicious Link Protections	Malicious file protections detect malicious files in communications and prevent users from accessing them.	Agencies should enable malicious link protections that prevent the device from receiving malicious links. When communications solutions enable end-to-end encryption, these protections may only be possible on the user endpoint device. When deploying endpoint protections, agencies should consider malicious link protections that can be applied to other methods of communication used by users (e.g., SMS).

Capability	Description	Use Case Guidance
Link Click-through Protections	Link click-through protections ensure that when a link is clicked, the requester is directed to a protection that verifies the security of the link destination before permitting access.	While malicious link protections can protect against known bad links, the protections can miss certain malicious links (e.g., if a nominally benign link becomes malicious). As remote users may not be accessing emailed links through agency boundary web protections, there may be no opportunity for protecting against these types of attacks. Agencies should consider link click-through protections that force the remote user's link access to traverse agency protections, even in situations where the remote user device is not using agency protections for its typical web access. When communications solutions enable end-to-end encryption, these protections may only be possible on the user endpoint device. When deploying endpoint protections, agencies should consider link click-through protections that can be applied to other methods of communication used by users (e.g., SMS).
Malicious File Protections	Malicious file protections detect malicious files in communications and prevent users from accessing them.	Agencies should enable malicious file protections for files sent or received through communications services. When communications solutions enable end-to-end encryption, these protections may only be possible on the user endpoint device, which potentially limits the types of file protections that can be applied to the files. Agencies should understand these limitations and ensure they are in alignment with agency risk tolerances.

7.2.10 Data Protection PEP Security Capabilities

Data protection is the process of maintaining the confidentiality, integrity, and availability of an agency's data consistent with their risk management strategy. It is important that agencies secure their data from corruption, compromise, or loss. Agencies should have processes and tools in place to protect agency data, prevent data exfiltration, and ensure the privacy and integrity of data, considering that data may be accessed from devices beyond the protections and perhaps

administration of agencies. Data protection capabilities must be considered and may be adapted for data stored and accessed at sanctioned agency cloud services, on agency-managed devices, as well as on remote devices that are not managed by an agency. Agencies should consider the sensitivity of data when applying rigor to these data protection PEP security capabilities. Policies, procedures, user training, and incident response may require adaptations to accommodate remote user access to services and data handling, storage, and uses. Table 13 lists the applicable Data Protection PEP Security Capabilities for the Remote User Use Case.

Table 13: Data Protection PEP Security Capabilities

Capability	Description	Use Case Guidance
Access Control	Access control technologies allow an agency to define policies concerning the allowable activities of users and entities to data and resources.	Agencies should consider the increased risk of loss, theft, or compromise of remote user devices when making authorization decisions on data access. Authorization decisions should account for the remote user device's security posture and its ability to provide protections commensurate to the sensitivity of the data. Agencies may consider restricting remote users' access to data according to the data sensitivity policies and their risk tolerance. Agencies should consider requiring MFA to access data to mitigate the effects of password compromise, device loss or theft, or device impersonation.
Protections for Data at Rest	Data protection at rest aims to secure data stored on any device or storage medium.	Agencies should ensure that any agency data stored on remote user devices is encrypted, either individually or via storage on encrypted areas of the devices, to mitigate the increased risk of loss or theft of remote user devices. Agencies may consider limiting the types of data provided to remote users or the ability for remote users to store agency data on the devices, especially if the agency does not have adequate assurance about the security posture of the remote user device.

Capability	Description	Use Case Guidance
Protections for Data in Transit	Data protection in transit, or data in motion, aims to secure data that is actively moving from one location to another, such as across the internet or through a private enterprise network.	Agencies should ensure that agency data is only made available to remote user devices through methods that ensure confidentiality and integrity commensurate to the sensitivity of the data.
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Agency DLP solutions should account for file exfiltration through remote user devices, with increased security rigor on file types, content, and volume of information permitted on remote user devices. Agency DLP may need to account for methods for accessing data, especially data stored in external environments, that bypass traditional infrastructure. Remote user technical enforcement may need to be supplemented with additional administrative controls addressing data handling and use when accessing services remotely.
Data Access and Use Telemetry	Data access and use telemetry identifies agency-sensitive data stored, processed, or transmitted, including those located at a service provider, and enforces detailed logging for access or changes to sensitive data.	When allowing remote users access to agency data, data access and use telemetry is especially important. Agencies should monitor remote users' accesses and changes to agency data to look for malicious activity or discrepancies in access patterns.
Data Labeling	Data labeling is the process of tagging data by categories to protect and control the use of data and identify the risk level associated with the data.	Agencies should ensure that data created by remote users is labeled in accordance with agency policies.
Data Inventory	Data inventory entails developing, documenting, and maintaining a current inventory of agency data.	Agency data inventories should track data that is stored on remote user devices or is accessed by remote users, including data accesses for data stored in agency campuses and agency cloud environments.

7.2.11 Identity PEP Security Capabilities

For agencies to securely allow remote users access to agency services, agencies must verify user identities, especially when performing potentially sensitive actions. To complicate this, there are multiple variables that can change when remote users attempt to connect to agency services, such as different network environments, different devices, and unusual times. Taking this into account, agencies should provide methods for remote users to further verify their identity when needed and provide a robust internal system to verify user identity. Table 14 lists the applicable Identity PEP Security Capabilities for the Remote User Use Case.

Table 14: Identity Protection PEP Security Capabilities

Capability	Description	Use Case Guidance
Adaptive Authentication	Adaptive authentication aligns the strength of the user or entity authentication mechanisms to the level of risk associated with the requested authorization.	Agencies should consider authentication strength according to user roles, device security and compliance, anomalous or suspicious login or user behavior, and the sensitivity of the requested access for remote users.
Entitlement Inventory	Entitlement inventory entails developing, documenting, and maintaining a current inventory of user and entity permissions and authorizations to agency resources.	Agencies may need to update their entitlement inventory to include authorizations for remote access as well as permissions and authorizations for remote users.
Secrets Management	Secrets management entails developing and using a formal process to securely track and manage digital authentication credentials, including certificates, passwords, and Application Programming Interface (API) keys.	Agencies should consider managing remote user secrets using systems that facilitate lifecycle management and secure storage and access. When developing workflows for managing secrets, agencies should account for the potential for remote users to lose access to internal agency services and how that might affect the secrets lifecycle. To account for potential loss or compromise of user secrets stored on remote user devices, agencies should consider mechanisms to revoke and replace compromised user secrets.

Capability	Description	Use Case Guidance
Behavioral Baselining	Behavioral baselining is capturing information about user and entity behavior to enable dynamic threat discovery and facilitate vulnerability management.	Agencies should understand and account for remote user behavior in agency environments to allow for the detection of anomalous or malicious behavior. When obtaining remote user baselines, agencies should consider accounting for activities performed in agency environments as well as where and how remote users access agency resources.
Enterprise Identity, Credential, and Access Management	Enterprise ICAM entails maintaining visibility into agency identities across agency environments and managing changes to those identities through a formal (preferably automated) process.	Agency enterprise ICAM solutions should integrate visibility and identity lifecycle management for remote users. Agencies should also account for risks associated with remote users by considering strong application of least privilege, limiting privileged accounts, and enabling detections for anomalous or malicious user and entity behavior.
Multi-factor Authentication	MFA entails using two or more factors to verify user or entity identity.	Agencies should, wherever possible, employ phishing-resistant MFA.[28] MFA solutions should allow for re-verification of identity when remote users seek to perform suspicious or sensitive actions. This will allow agencies to minimize opportunities for lateral movement or privilege escalation from account compromise. Where MFA is used by remote users, the authentication processes should account for situations where the remote user does not have connectivity to centralized services.

[28] "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," Office of Management and Budget M-22-09 (2022). https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

Capability	Description	Use Case Guidance
Continuous Authentication	Continuous authentication entails validating and re-authenticating identity through the lifecycle of entity interactions.	Agencies should employ solutions that re-verify identity when remote users seek to perform sensitive actions or when anomalous or suspicious behavior is detected. This includes aligning the strength of authentication for the re-verification according to user roles, device security and compliance, and the sensitivity of the requested action.

8. TELEMETRY REQUIREMENTS

As agencies allow remote users to connect more directly to external services, visibility by CISA must be preserved through information sharing. Figure 8 shows the conceptual architecture of the Remote User Use Case, with the telemetry requirements added as lines on certain data flows. These lines, depicted in Figure 8, indicate when an agency must share telemetry with CISA. CISA may require internal telemetry to be collected. The requirements for sharing telemetry data with CISA are only applicable to the data flows between the remote user and the web and CSPs. Consult the NCPS program[29] and CDM program[30] for further details.

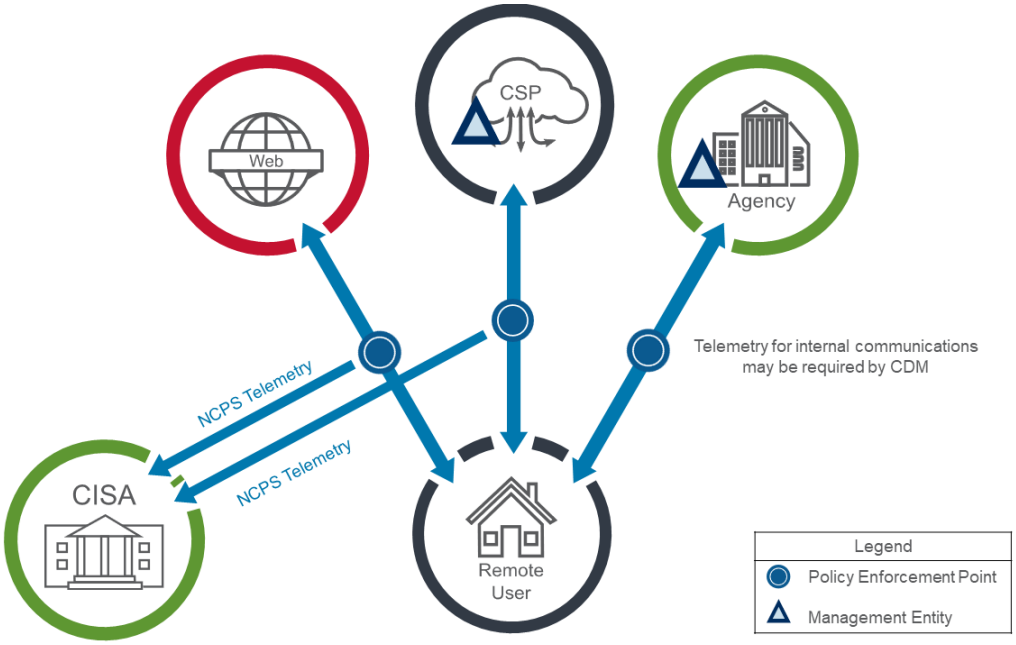


Figure 8: Remote User Telemetry Sharing with CISA

8.1 TELEMETRY CONSIDERATIONS

Providing telemetry about remote user devices can present some challenges compared to traditional on-premises deployments. On-premises deployments often route all traffic through centralized locations which enables a small number of collection points to provide telemetry about all agency traffic. If remote users use VPN or VDI for all external access, their telemetry may be provided by the traditional collection infrastructure. However, if a remote user can bypass the traditional collection infrastructure when accessing agency services, especially those deployed in cloud environments, or when accessing untrusted services in the web, the agency may need to augment its telemetry collection to maintain visibility in accordance with OMB M-21-31.[31] When using other data sources to augment the telemetry for remote users, agencies will need to consider the additional information available in these other sources which may enrich their traditional visibility, and the potential privacy impacts they may have.

[29] "National Cybersecurity Protection System (NCPS)," https://www.cisa.gov/national-cybersecurity-protection-system-ncps.
[30] "Continuous Diagnostics and Mitigation (CDM)," https://www.cisa.gov/cdm.
[31] "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," Office of Management and Budget M-21-31 (2021). 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.

For remote user devices, agencies often collect telemetry from the devices themselves, including telemetry about the overall state of the device and telemetry about its interactions with services, trusted or untrusted. However, the remote nature of the devices means that they may only have intermittent access to be able to provide that telemetry. As this telemetry collection relies on the correct functioning of the remote user device, the higher risk associated with remote devices may make it prudent to use telemetry collected from other sources to increase the confidence in the telemetry provided by the remote user devices.

Beyond collecting telemetry from the remote user devices, agencies may also be able to collect relevant telemetry about remote user devices from the vantage point of agency services, whether on-premises or deployed in cloud environments. While relevant telemetry may need to be integrated from a variety of services to provide a comprehensive view of the remote user device's actions, this vantage point can provide additional fidelity by providing a telemetry source that is independent of the remote user device itself. This is especially important if the agency is unable to retrieve telemetry from the remote user device itself (e.g., it's unmanaged, it's BYOD, etc.). However, this vantage point may provide only limited insights into the remote user device itself and cannot provide any telemetry about a remote user device's access to untrusted services.

Under some deployment models (e.g., VPNs, CASB, or other SECaaS, etc.), remote user devices may route their traffic through common infrastructure that enables the collection of relevant telemetry. Similar to the collection of telemetry from the agency services, this vantage point allows for the collection of telemetry with limited dependence on the remote user devices. Unlike the agency service vantage point, this collection model may be able to expand the collection of telemetry to include interactions with non-agency services. While this deployment model may have the expectation that remote user devices employ technologies that route their traffic through the common infrastructure, agencies should account for whether the devices can be used to access services, whether trusted or untrusted, without employing those technologies (e.g., accessing the web from a remote user device without first establishing a VPN to the agency).

Agencies may need to obtain telemetry from a variety of vantage points to provide a view of a remote user device equivalent to what might be available from an on-premises deployment. While it may be possible to provide the telemetry directly from each of these locations, the wide variety of endpoints, especially if the remote user device is providing telemetry, along with the diverse formats of telemetry and concerns about privacy may mean that an agency should consider collecting, processing, integrating, and filtering the telemetry before providing it for external consumption.

9. CONCLUSION

The Remote User Use Case defines how network and multi-boundary security should be applied when an agency user can access agency resources, either agency-hosted or in cloud environments, from outside agency network boundaries. This document provides guidance on how an agency can configure its remote user data flows and apply relevant TIC security capabilities. It considers three network security patterns:

- Secure remote user access to agency campus,
- Secure remote user access to agency-sanctioned CSPs, and
- Secure remote user access to web.

APPENDIX A – GLOSSARY AND DEFINITIONS

This glossary contains terms and definitions that are used across the TIC documents and not necessarily applicable to all use cases.

Boundary: A notional concept that describes the perimeter of a zone (e.g., mobile device services, general support system (GSS), Software-as-a-Service (SaaS), agency, etc.) within a network architecture. The bounded area must have an information technology (IT) utility.

Internet: The internet is discussed in two capacities throughout TIC documentation:

1. A means of data and IT traffic transport.
2. An environment used for web browsing purposes, referred to as "Web."

Managed Trusted Internet Protocol Services (MTIPS): Services under GSA's Enterprise Infrastructure Solutions (EIS) contract vehicle that provide TIC solutions to government clients as a managed security service. It is of note that the EIS contract is replacing the GSA Networx contract vehicle that is set to expire in Fiscal Year (FY) 2023.

Management Entity (MGMT): A notional concept of an entity that oversees and controls security capabilities. The entity can be an organization, network device, tool, service, or application. The entity can control the collection, processing, analysis, and display of information collected from the policy enforcement (PEPs), and it allows IT professionals to control devices on the network.

National Cyber Protection System (NCPS): An integrated system-of-systems that delivers a range of capabilities, including intrusion detection, analytics, intrusion prevention, and information sharing capabilities that defend the civilian Federal Government's information technology infrastructure from cyber threats. The NCPS capabilities, operationally known as EINSTEIN, are one of several tools and capabilities that assist in federal network defense.

Policy Enforcement Point (PEP): A security device, tool, function, or application that enforces security policies through technical capabilities.

Policy Enforcement Point Security Capabilities: Network-level capabilities that inform technical implementation for relevant use cases.

Reference Architecture (RA): An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.

Risk Management: The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Tolerance: The level of risk or degree of uncertainty that is acceptable to organizations and is a key element of the organizational risk frame. An organization's risk tolerance level is the amount of corporate data and systems that can be risked to an acceptable level.

Security Capability: A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals). Security capabilities help to define protections for information being processed, stored, or transmitted by information systems.

Security Pattern: Description of an end-to-end data flow between two trust zones. Security patterns may have an associated set of security capabilities or guidance to secure the data flow along with one or more of the zones.

Seeking Service Agency (SSA): An agency that obtains TIC services through an approved Multi-Service TICAP.

Security Information and Event Management (SIEM): An approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system.

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

TIC: The term "TIC" is used throughout the Federal Government to denote different aspects of the TIC initiative; including the overall TIC program, a physical TIC access point (also known as a Traditional TIC), and a TIC Access Provider (TICAP – see below). This document refers to TIC as an adjective or as the Trusted Internet Connections initiative.

TIC Access Point: The physical location where a federal civilian agency consolidates its external connections and has security controls in place to secure and monitor the connections.

TIC Access Provider (TICAP): An agency or vendor that manages and hosts one or more TIC access points. Single Service TICAPs serve as a TIC Access Provider only to their own agency. Multi-Service TICAPs also provide TIC services to other agencies through a shared services model.

TIC Initiative: Program established to optimize and standardize the security of individual external network connections currently in use by the Federal Government, to include connections to the internet. Key stakeholders include CISA, OMB, and GSA.

TIC Overlay: A mapping from products and services to TIC security capabilities.

TIC Use Case: Guidance on the secure implementation and/or configuration of specific platforms, services, and environments. A TIC use case contains a conceptual architecture, one or more security pattern options, security capability implementation guidance, and CISA telemetry guidance for a common agency computing scenario.

Trust Zone: A discrete computing environment designated for information processing, storage, and/or transmission that dictates the level of security necessary to protect the traffic transiting in and out of a zone and/or the information within the zone.

Unified Communications and Collaboration (UCC): A collection of solutions designed to facilitate communication and collaboration, including in real-time, such as required by remote work or collaboration between locations.

Universal Security Capabilities: Enterprise-level capabilities that outline guiding principles for TIC use cases.

Web: An environment used for web browsing purposes. Also see Internet.

Zero Trust: A security model based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter.

APPENDIX B – RELATED FEDERAL GUIDELINES

The following list of documents include the most recent version of the guidance documents available at the time of this publication, including drafts.

Cybersecurity and Infrastructure Security Agency, *Capacity Enhancement Guides for Federal Agencies: Implementing Strong Authentication*, October 2020.

Cybersecurity and Infrastructure Security Agency, *Cloud Security Technical Reference Architecture, Version 2.0*, June 2022.

Cybersecurity and Infrastructure Security Agency, *Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*, November 2021.

Cybersecurity and Infrastructure Security Agency Telework Guidance and Resources, https://www.cisa.gov/telework.

Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model, Version 2.0*, April 2023.

Department of Defense, *Zero Trust Reference Architecture, Version 2.0*, July 2022.

Cybersecurity and Infrastructure Security Agency. *Extensible Visibility Reference Framework Guidebook Request for Comment Draft*, April 2022.

Federal Information Security Modernization Act of 2014 (P.L. 113-283), codified in relevant part in 44 U.S.C. §§ 3551-8.

Federal Information Security Modernization Act (P.L. 113-283), December 2014,

National Institute of Standards and Technology Special Publication 800-46, Revision 3 (Draft), Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, September 2020.

National Institute of Standards and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, December 2020.

National Institute of Standards and Technology Special Publication, 800-63-3, Digital Identity Guidelines, June 2017.

National Institute of Standards and Technology Special Publication 800-83, Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, July 2013.

National Institute of Standards and Technology Special Publication 800-114, Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security, July 2016.

National Institute of Standards and Technology Special Publication 800-124, Revision 2 (Draft), Guidelines for Managing the Security of Mobile Devices in the Enterprise, March 2020.

National Institute of Standards and Technology Special Publication 800-207, Revision 1, Zero Trust Architecture, August 2020.

National Institute of Standards and Technology, Special Publication 800-210, General Access Control Guidance for Cloud Systems, July 2020.

Cybersecurity and Infrastructure Security Agency, *Secure Cloud Business Applications Microsoft 365 Baselines Draft*, December 2022.

Cybersecurity and Infrastructure Security Agency. *Secure Cloud Business Applications Technical Architecture Request for Comment Draft,* April 2022.