TRUSTED INTERNET CONNECTIONS 3.0 INTERIM TELEWORK GUIDANCE

INTRODUCTION

Purpose

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is monitoring the evolving coronavirus disease 2019 (COVID-19) situation closely, taking part in interagency and industry coordination calls, and working with critical infrastructure partners to prepare for possible disruptions to critical infrastructure that may stem from widespread illness. As federal civilian agencies respond to the COVID-19 situation, the number of federal agency employees working remotely has increased dramatically. In order to support agencies as they respond to this surge in teleworking, CISA is issuing this interim Trusted Internet Connections (TIC) guidance[1] to help agencies leverage existing resources to secure their networks.

The purpose of this document is to help federal civilian agencies address the telework surge concerns by:

- Providing awareness that the security patterns outlined under Agency Teleworker Options 1 and 2 (below) align to TIC architecture capabilities as presented in the draft TIC 3.0 guidance (December 2019).
    - Agencies should ensure that appropriate data sharing is maintained with Agency Security Operations Centers.
    - Agencies should be prepared to discuss the availability of log and telemetry features in order to determine what relevant information will need to be provided to CISA for cybersecurity analytical purposes.
- Informing agencies that the interim guidance provided under Agency Teleworker Option 3 provides additional temporary relief with additional security patterns.
- Suggesting security capabilities for agencies to consider when creating or expanding their teleworking platforms.
- Allowing vendors to map the cybersecurity capabilities provided by their services to the TIC security capabilities that support secure teleworking.

This guidance reflects the authorities given to agencies outlined in Office of Management and Budget (OMB) Memorandum 19-26: *Update to the TIC Initiative*. This document is intended to be architecture-agnostic and broadly support a wide spectrum of architectural implementations (e.g., virtual private network (VPN) users, virtual desktop interfaces (VDI), zero trust environments, etc.). It is not intended to be prescriptive; instead, it should be leveraged by agencies and adapted for practical teleworking scenarios. As agencies move away from traditional network

[1] For more information about the TIC program, please see: https://www.cisa.gov/trusted-internet-connections. For OMB guidance on COVID-19, please see: https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-17.pdf.

architectures for remote access, there will be a greater reliance on authentication mechanisms to validate the remote user.

This document will begin by explaining the objectives underpinning the TIC program. Next, it will present the security pattern for teleworkers interacting with agency-sanctioned cloud service provider (CSP) resources. It will then introduce the reader to TIC security capabilities and present the list of suggested capabilities to implement for telework. The document includes an appendix with an explanation of how vendor overlays can be used to map vendor service offerings to proposed TIC security capabilities and presents a template for a vendor mapping.

Scope

Teleworkers require access to resources on the agency campus, agency-sanctioned cloud services, and on the public web. Each of these security patterns presents unique risks and corresponding security capabilities for appropriate use. This document will focus on TIC 3.0 adaptations for communication between teleworkers and agency-sanctioned cloud services. Teleworker communications with agency campus hosted resources and with web entities should continue to follow established agency protections. This guidance directly supports OMB Memorandum 20-19, "Harnessing Technology to Support Continuity."[2]

Constraints and Assumptions

This document is only intended to address the current teleworking surge. It is not intended to be part of the TIC 3.0 document set or support a TIC 3.0 use case; it will be deprecated at the end of 2020. The guidance is not intended to be comprehensive and should not be interpreted as a use case nor reference architecture. Agencies can refer to the TIC 3.0 document set for more details on the TIC program and objectives, additional TIC 3.0 guidance, and clarification of TIC terminology used throughout this document. This interim guidance will be integrated into the TIC 3.0 Remote User Use Case at a later date.

The COVID-19 situation presents unique cybersecurity threats, and agencies must consider these unique threats when securing their platforms. This document identifies a subset of the security capabilities detailed in the TIC 3.0 Security Capabilities Handbook that are applicable to the current telework surge and can be used to prevent, mitigate, and detect some of these emerging threats. This document also introduces new TIC security capabilities that are unique to telework. The full set of TIC security capabilities can be found in the TIC 3.0 TIC Security Capabilities Handbook.

This document is only intended to address scenarios in which agency users connect remotely to agency-sanctioned cloud environments. Any traffic to the public internet (i.e., public web traffic) must still be routed through EINSTEIN sensors, the operational capabilities of the National Cybersecurity Protection System (NCPS) program[3]. When in doubt, agency traffic should be routed through EINSTEIN sensors.

Vendors will be responsible for mapping their service offerings to the suggested TIC objectives and security capabilities. Agencies and vendors should work together to identify appropriate implementation approaches that focus on improving employment of capabilities and services in alignment with agency risk tolerances.

Agencies, in consultation with appropriate vendors, will coordinate the expansion of cloud and collaboration services that deviate from existing reference architectures to ensure that CISA programs are notified. Agencies should be prepared to discuss the availability of log and telemetry features in order to determine what relevant information will need to be provided to CISA for cybersecurity analytical purposes.

---

[2] https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-19.pdf
[3] https://www.cisa.gov/national-cybersecurity-protection-system-ncps

Agencies should leverage policies that permit security enforcement on remote user and client-side devices such as Bring Your Own Device (BYOD).

TIC OBJECTIVES

To protect these dispersed assets, the TIC program defines encompassing security objectives[4] to guide agencies in securing their network traffic. The objectives intend to limit the potential impact of a cybersecurity event. The TIC 3.0 Interim Telework Guidance is intended to support fulfillment of the following objectives that guide TIC 3.0:

TIC Program Security Objectives

Objective	Description
Manage Traffic	Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny.
Protect Traffic Confidentiality	Ensure only authorized parties can discern the contents of data in transit; sender and receiver identification and enforcement.
Protect Traffic Integrity	Prevent alteration of data in transit; detect altered data in transit.
Ensure Service Resiliency	Promote resilient application and security services for continuous operation as the technology and threat landscape evolve.
Ensure Effective Response	Promote timely reaction and adapt future response to discovered threats; policies defined and implemented; simplified adoption of new countermeasures.

How Agencies Can Use this Document

This document is intended to provide general guidance to agencies to increase telework and collaboration capacity to meet the growing demands on their existing services. Increasing capacity and capabilities for remote telework and collaboration may require an increase in existing services such as internet service provider (ISP) bandwidth, VPN, and cloud. In some cases, agencies may find that there is a need to deploy new cloud services and authorize the use of non-government furnished equipment (non-GFE) or BYOD to facilitate access to remote resources to meet demands. As agencies are considering options, licensing upgrades many be necessary to support a broader set of cybersecurity tools and services to support situational awareness and manage risks.

In the spirit of this guidance, agencies, in consultation with vendors, should review service provider overlays to understand coverage as well as gaps in TIC security capabilities and security policies that may need to be applied to govern the use of non-GFE/BYOD. Overlays can be used to assess risks associated with expanding and adding new services in the context of availability, confidentiality, and integrity as well as relevant threats and attack surface exposure based on changes to their environment. To the extent practical, agencies should assess risks associated with broadening the use of cloud and collaboration services to ensure that due care as well as due diligence is applied to these changes in their respective information technology (IT) and user environments. CISA will not participate in the mapping process. CISA will also not attest to nor validate the strength of the vendor services nor the implementation

[4] TIC 3.0 Program Guidebook, Pg. 10-11.

approaches by agencies.

OTHER CISA PROGRAMS

Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM)[5] Program Management Office (PMO) is in the process of evaluating where the program can adjust based on recent feedback received from agencies and CDM system integrators. CDM PMO is also conducting various testing activities within the National Cybersecurity Center of Excellence (NCCOE) CDM generic instance lab to evaluate and understand security capabilities in the cloud. The testing may help agencies understand the risks associated with the expansion of telework capabilities that have affected all agencies within the federal civilian executive branch.

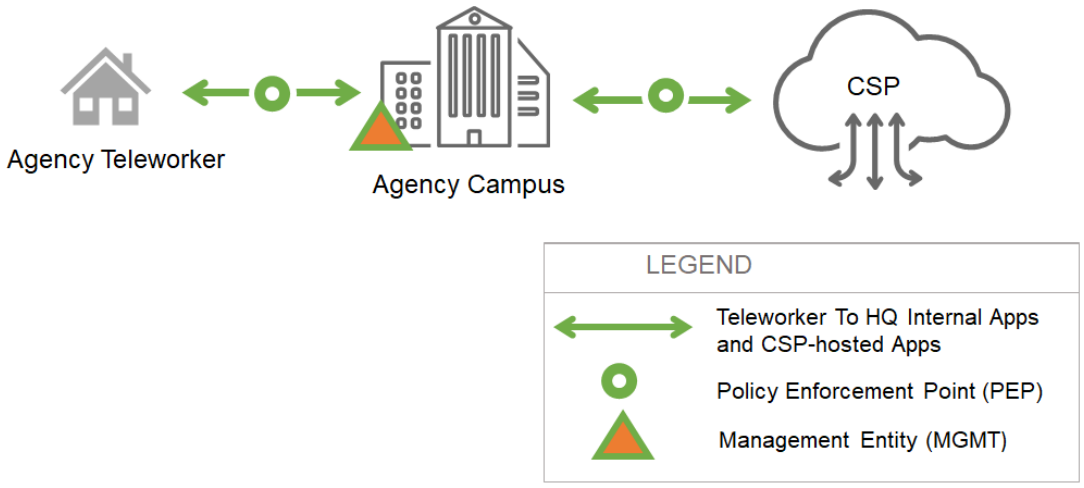
[5] https://www.cisa.gov/cdm

TELEWORKER TO CSP SECURITY PATTERN

Teleworkers require access to resources on 1) the agency campus, 2) agency-sanctioned cloud services, and 3) the public web. Each of these security patterns presents unique risks and corresponding security capabilities for appropriate use. This document will focus on TIC 3.0 adaptations for communication between teleworkers and agency-sanctioned cloud services. Teleworker communications with agency campus hosted resources and with web entities should continue to follow established agency protections.

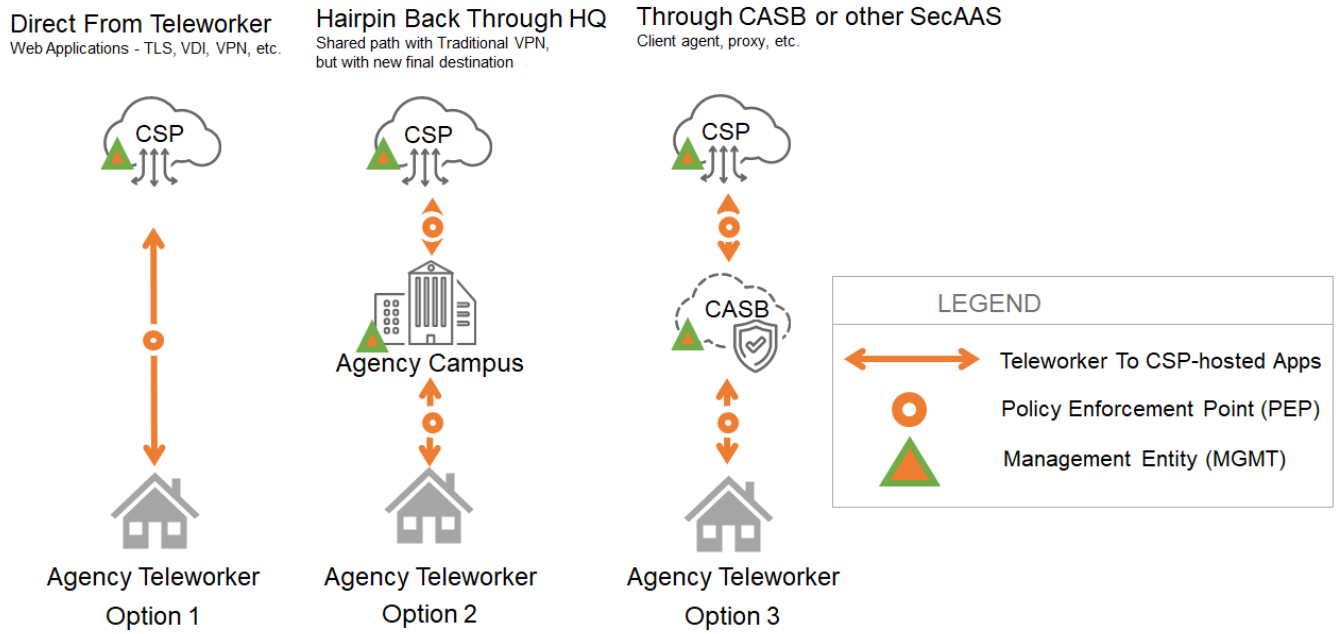
Traditionally, when teleworkers require access to agency-sanctioned cloud services, they first establish a trusted connection to agency campus resources (e.g. VPN or VDI). Aggregating all teleworker traffic through a single location facilitates security policy enforcement and protection parity at a central location. As shown in Figure 1, this security pattern also enables teleworkers and agency campus users to leverage the same connectivity to CSP resources (both conveyance and policy enforcement point (PEP)). However, teleworker connections to agency campus concentrators at scale requires additional resources, incurs greater costs, and decreases performance.

FIGURE 1 - TRADITIONAL TELEWORKER ACCESSING CSP RESOURCES SECURITY PATTERN

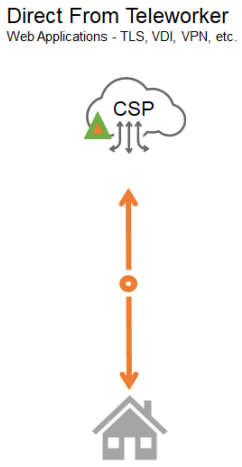


TIC 3.0 promotes connection methods that permit teleworkers to access agency-sanctioned CSP resources while preserving policy enforcement parity and accommodating various risk tolerances. These connection types are illustrated in the security pattern options shown below in Figure 2. Detailed descriptions of each option follow.

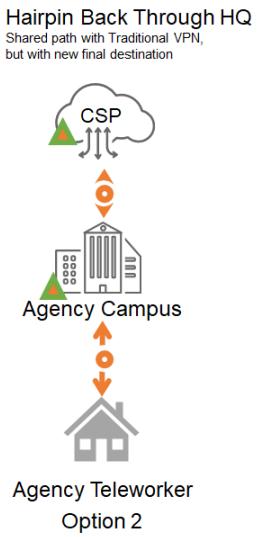
FIGURE 2 - ALTERNATIVE SECURITY PATTERNS FOR TELEWORKER ACCESSING CSP RESOURCES



Agencies should ensure that teleworker traffic destined for the CSP is properly constrained to sanctioned destinations. Agencies should also ensure that teleworkers do not connect to unsanctioned resources (e.g., when alternate destinations are unsanctioned tenancies hosted on the same CSP).



In the first option, teleworkers can access CSP resources directly. Policy enforcement placement and protections are applied at the CSP and on teleworker resources. Capabilities may be duplicated with those traditionally handled by agency campus services so long as policy enforcement parity is ensured. CSP resources must also consider eligibility enforcement as this may be less stringent than single-source protections traditionally available. Teleworker resources may also include systems which are not managed by agencies (e.g. BYOD) and may not be suitable for performing some policy enforcement capabilities.



Option 2 aligns with traditional mechanisms for accessing CSP resources. Teleworkers first establish a protected connection to the agency campus and then make connections to CSP resources through that channel. Policy enforcement can be performed at the teleworker, agency campus, and CSP. Teleworkers may establish the connection to agency campus resources for additional business functions alongside connections to the CSP. This option facilitates common connectivity to CSP resources for both campus and telework users. This may include dedicated connections to the CSP with enhanced performance, security, or other enhancements. Eligibility enforcement for CSP access can rely upon connection origin as an additional attribute for policies. Teleworkers may see reduced performance due to increased network latency, stacked network encryption, increased likelihood for network congestion, concentrator licensing bottlenecks, and/or other resource exhaustion. When teleworkers do not require access to agency campus resources for business operations, their connections may simply be an unnecessary burden on concentrator capacity.

Through CASB or other SecAAS
Client agent, proxy, etc.

Agency Teleworker

Option 3 permits connectivity from teleworkers to agency-sanctioned CSP resources through a cloud access security broker (CASB) or other security-as-a-service (SECaaS) provider. Policy enforcement placement options include teleworker, CASB, and CSP resources. Policy enforcement parity between agency campus and teleworker users can be simplified when both utilize the same CASB or SECaaS provider. Teleworker systems can have their traffic directed to the CASB through client agents, proxy settings, and/or DNS means. The addition of a CASB or SECaaS policy enforcement point may increase the CSP capability precision, as whitelists can be authored to constrain connections to those originating at the CASB. This positions agency-sanctioned CSP access eligibility enforcement partially upon the CSP and partially upon the CASB, offering a separation of duties. When teleworkers require connectivity to both CSP and agency campus resources there must be a policy and enforcement for concurrent or mutually exclusive connectivity and the conditions under which each apply.

TIC SECURITY CAPABILITIES LIST FOR TELEWORK

Universal Security Capabilities

Universal 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 capabilities based on federal guidelines and risk tolerance. The table below provides: (1) a list of the universal security capabilities that apply to remote teleworking, (2) a description of each capability, (3) a mapping of each capability to relevant National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[6] categories, and (4) specific implementation guidance for agencies to consider during a telework surge.

While universal capabilities are broadly applicable, the circumstances and threats associated with the telework surge require agencies to consider the workforce shift and security challenges that must be addressed. **Each of these universal capabilities should be reviewed by agencies as they consider how a surge in telework affects changes to their enterprise.**

Universal Security Capabilities

Capability	Description	NIST CSF Mapping	Telework-Specific Implementation Guidance
Backup and Recovery	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.	PR.IP, PR.DS, RS.MI, RC.RP	Ensure that relevant data is being maintained. If possible, back up agency devices.
Central Log Management with Analysis	Storing telemetry needed to discover and respond to malicious activity in a manner that facilitates security analysis and data fusion.	ID.AM, PR.PT, DE.AE, RS.AN	Log management should include agency user device logs and Service Logs. Activate additional logging and increase log alerts to detect new malicious activity related to the telework surge. Ensure adequate storage for additional logs. Regularly review logs.
Configuration Management	Implementing a formal plan for documenting, managing changes to the environment, and monitoring for deviations.	ID.BE, PR.DS, PR.IP, PR.MA	Consider Device Compliance for mobile devices and device conformance with agency policies during connection initiation.
Incident Response Plan and Incident Handling	Documenting and implementing a set of instructions or procedures to detect, respond to, limit consequences of malicious cyberattacks, and restore the	ID.GV, ID.RA, PR.IP, DE.DP, DE.AE, RS.RP,	Account for remote devices. Track users, especially doing things inconsistent with typical telework. Monitor shared services for misuse and breach and adapt response plans and activities accordingly.

[6] https://www.nist.gov/cyberframework

Capability	Description	NIST CSF Mapping	Telework-Specific Implementation Guidance
	integrity of the network and systems.	RS.CO, RS.AN, RS.MI	
Inventory	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 prevented from gaining access.	ID.AM, PR.DS, PR.AC, PR.DS, PR.IP	Account for increased use of virtual services. Where possible, track users' devices and their respective compliance.
Least Privilege	Designing the security architecture such that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	ID.AM, PR.AC, PR.IP, PR.PT, DE.CM	Agency users' access to agency services and data should take into account the security of the device the user is using to access the service or data, enabling higher levels of access to users with more secure devices.
Secure Administration	Performing administrative tasks in a secure manner, using secure protocols.	PR.MA	Consider requisite changes to remote desktop support services, device patch management across remote connections, and local user privilege level modifications.
Strong Authentication	Verifying the identity of users, devices or other entities through rigorous means (e.g., multi-factor authentication) before granting access.	PR.AC	Ensure users are authenticated to all agency servers using MFA, in accordance with OMB M-19-17[7]. If MFA is unsupported by a service, strong password policies should be in place with the service, ensuring that no passwords are reused if agency users need access to multiple services that do not support MFA. As agencies move away from traditional network architectures for remote access, there will be a greater reliance on authentication mechanisms to validate the remote user.
Time Synchronization	Coordinating clocks on all systems (e.g., servers, workstations, network	PR.IP	Agency user devices should be synchronized. However, given the difficulties in ensuring clock synchronization across all devices that agency

[7] OMB Memo M-19-17, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," May 21, 2019.

Capability	Description	NIST CSF Mapping	Telework-Specific Implementation Guidance
	devices) to enable accurate comparison of timestamps between systems.		users may use, agency user actions should be logged from the service side, where timestamp accuracy can be more readily ensured.
Vulnerability Assessment	Proactively working to discover vulnerabilities, including the use of both active and passive means of discovery, and taking action to mitigate discovered vulnerabilities.	ID.RA, PR.IP, DE.AE, DE.CM, DE.DP	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.
Auditing and Accounting	Capturing business records, including logs and other telemetry, and making them available for auditing and accounting as required.	ID.SC, PR.AC, PR.PT	Cloud service licensing, activity, and billing may require adaptation to existing tracking mechanisms. Agencies should ensure compatibility and interoperability to minimize visibility gaps.
Resilience	Ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.	ID.BE, PR.PT	Agencies should proactively work to ensure the agency services have the capability to scale as necessary to handle telework by agency users.
Enterprise Threat Intelligence	Obtaining threat intelligence from private and government sources and implementing mitigations for the identified risks.	ID.RA, DE.AE, DE.CM, DE.DP	Agencies should seek out and adopt any new threat intelligence feeds which align with new services or delivery mechanisms deployed.
Situational Awareness	Maintaining effective awareness, both current and historical, across all components.	ID.AM, ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.CO	Maintain awareness from agency services. Maintain awareness of agency users. Agencies should seek integration of any new CSP telemetry into centralized situational awareness tools.
Dynamic Threat Discovery	Using dynamic approaches (e.g., heuristics, baselining, etc.) to discover new malicious activity.	ID.RA, DE.AE, DE.CM, DE.DP	Track agency user use of agency services or data, include device information if possible, to look for changes or discrepancies.

Capability	Description	NIST CSF Mapping	Telework-Specific Implementation Guidance
Policy Enforcement Parity	Consistently applying security protections and other policies, independent of the conveyance mechanism used.	PR.DS, PR.IP, PR.MA	Agencies should ensure integrated desktop, mobile, and remote policies align. Care must be taken to ensure any new teleworker endpoint protections align with established agency risk tolerances.
Effective Use of Shared Services	Employing shared services, where applicable, that can be individually tailored, measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external as well as internal to the service provider.	ID.AM, ID.GV, ID.RM, ID.SC, PR.AT, RS.CO	Shared services can improve teleworker resource usability, increase service availability and resilience, and enhance user experience. Agencies should give careful consideration to security capabilities when selecting shared service providers.
Integrated Desktop, Mobile, and Remote Policies	Defining polices such that they apply to a given agency entity no matter its location.	ID.AM, PR.AC, PR.DS, PR.IP, PR.MA	Agencies should employ methods allowing user policies to be defined in accordance with the agency's abilities to enforce policies. If an agency policy allows a user to make use of a device that the agency cannot enforce policies on, the policies 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.

Policy Enforcement Point Capabilities

Policy Enforcement Point (PEP) capabilities are network-level capabilities that inform technical implementation for a given use case, such as teleworker communication with agency-sanctioned CSPs here. PEP capabilities are divided into groups and fulfilled by applications, devices, or services identified in TIC Use Cases and TIC Overlays. From the existing TIC 3.0 Security Capabilities Handbook, the PEP capability groups applicable to telework correspond to the following security functions:

- Files,
- Email,
- Networking,
- Resiliency,
- DNS,
- Intrusion Detection, and
- Enterprise.

The increased surge in telework use also requires consideration of the following new PEP capability groups:

- Unified Communications and Collaboration, and

- Data Protection.

The PEP capability listing is not exhaustive. Additional security capabilities may be deployed by agencies to reflect their risk tolerances, early adoption of security capabilities, maturity level of existing cyber programs, etc. In addition to telework-specific guidance for each functional group of security capabilities, the following tables provide: (1) a list of PEP capabilities, (2) a description of each capability, and (3) a mapping to relevant NIST CSF categories.

Files

With agency users operating outside the traditional agency boundary, the agency's anti-malware deployment model may need to change. Anti-malware technologies should be, if possible, deployed to the devices that agency users are using, whether personally-owned or government furnished. These protections, however, may not provide any telemetry back to the agency, which may increase the reliance on anti-malware technologies on the agency side. These should be deployed any time an agency service is transiting a file to or from an agency user (e.g. email, web client proxying, etc.).

Files Capabilities

Capability	Description	NIST CSF Mapping
Anti-malware	Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.	PR.DS, PR.PT, DE.CM, DE.DP, RS.MI

Email

Telework environments, can present significant challenges associated with mitigating email-based threats (e.g., phishing). This challenge is amplified by the reality that agencies have limited visibility or control over remote user devices as the email service may be the only opportunity for meaningfully policy enforcement. For instance, when mail agents are on an agency campus the agency may be able supplement email protections with secure web gateway, anti-malware, intrusion detection systems, and other network and host-based protections. When remote users are accessing email from remote locations, the same protections may no longer be available at the same enforcement and performance levels. Telework may also increase the reliance upon email services for information exchange, as users may not be able to leverage alternative means to the same degree as when workers were on site. 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.

Email Capabilities

Capability	Description	NIST CSF Mapping
Anti-phishing Protections	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	PR.AT, PR.PT, DE.CM
Data Loss Prevention	Data Loss Prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	PR.DS
Encryption for Email Transmission	Email Services are configured to use encrypted connections, when possible, when interacting with Clients and other Email Servers.	PR.PT, PR.DS

Capability	Description	NIST CSF Mapping
Malicious URL Protections	Malicious URL Protections detect malicious URLs in emails and prevent users from accessing them.	PR.PT, DE.CM
URL Click-Through Protection	URL Click-Through Protections ensures that when a URL from an email is clicked, the requester is directed to a protection that verifies the security of the URL destination before permitting access.	PR.PT, DE.CM
NCPS E^{3}A Email Protections	NCPS E^{3}A is an intrusion prevention capability, provided by DHS, that includes an Email Filtering security service.	PR.PT, DE.CM

Networking

With access to services primarily coming from external parties, agencies have much less control over end user devices which may make it prudent to assume end devices end up compromised. Segmenting the network to limit users' access to only the services, or data that they require can help mitigate these risks. When endpoints require concurrent connections to multiple destinations it is known as "split tunneling." Network segmentation of end user devices may include consideration for "split tunneling" when requiring connections to both agency campus resources and agency-sanctioned CSP services. Care must be taken to ensure data flows are forwarded to appropriate destinations and decision points for making this determination are not easily bypassed or manipulated. Agency-sanctioned CSP services must also preserve proper network segmentation to ensure least privilege principles are enacted.

Networking Capabilities

Capability	Description	NIST CSF Mapping
Network Segmentation	Network Segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.	PR.AC
Micro-segmentation	Micro-segmentation divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data.	PR.AC, PR.DS, PR.IP, PR.PT

DNS

For telework to be effective, agency users need to trust their agency domain names, the domain names are resolving, and that the domain names point to the appropriate resources. To enable users to validate the domain names, agencies need to host those domain names in DNS services that provide domain name system security extension (DNSSEC) capabilities. Agency users may be connecting to these agency services from a variety of network environments, some of which may not support DNSSEC and some of whom may have been compromised. To account for these, it may be prudent for agency users to manually specify DNS providers that support DNSSEC. When feasible, remote workers should utilize name resolution services with the same protections as endpoints on the agency campus. Teleworker endpoints may not be managed assets of the agency, reducing the ability of agencies to enforce name resolution protection consistency.

DNS Capabilities

Capability	Description	NIST CSF Mapping
DNS Blackholing	DNS Blackholing protections are a form of blacklisting that protect clients from accessing malicious domains by responding to DNS queries for those domains.	PR.PT
DNSSEC for Agency Clients	DNSSEC protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated.	PR.PT
DNSSEC for Agency Domains	DNSSEC protections ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution the domain names.	PR.PT
NCPS E^{3}A DNS Protections	NCPS E^{3}A is an intrusion prevention capability, provided by DHS, that includes a DNS Sinkholing security service.	PR.PT

Intrusion Detection

An environment that is primarily telework has a different set of requirements than a traditional on-premises environment. With access to services primarily coming from external parties, agencies retain much less control over end user devices, especially in being able to perform post-incident forensics. With less visibility and control in users' devices, it may be prudent to assume they may end up compromised and to 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 end user's device, or look for anomalies in accessing data or use of services to detect malicious activity from the server side). Access control rules may be able to further restrict connections based on shelter-in-place or prohibited travel rules enacted by local government authorities. These temporary location restrictions may enable discovery of misused or stolen credentials based on multiple concurrent logins or impossible travel attributes.

Intrusion Detection Capabilities

Capability	Description	NIST CSF Mapping
Adaptive Access Control	Adaptive Access Control technologies factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.	PR.AC, DE.CM
Endpoint Detection and Response	Endpoint Detection and Response tools combine endpoint and network event data to aid in the detection of malicious activity.	DE.AE, DE.CM, RS.AN

Enterprise

Effective telework often depends on users' ability to remotely access an agency network, agency managed application, or an agency computer. There are numerous methods for doing so, including VPN, mobile application containers, and remote desktop access. Given the wealth of access to internal services that these tools can provide along with the need to make them available to users connecting via the internet, extra care needs to be used to ensure that these entry points are well-secured, including being up to date with security patches. To mitigate the impact of users having their

credentials stolen, these services should only be available using secure protocols (e.g. IPsec, TLS) and should use Multi-Factor Authentication (MFA). Mechanisms should also be in place to revoke access, clear the remote endpoint of agency data, and/or collect security telemetry. Teleworker endpoints which are not owned or managed by agencies may not be suitable for VPN or remote desktop access but may rely upon application or enterprise container capabilities for desired functionality.

Enterprise Capabilities

Capability	Description	NIST CSF Mapping
VPN	Virtual private network solutions provide a secure communications mechanism between networks that may traverse across unprotected or public networks.	PR.AC, PR.DS, PR.IP, PR.MA, PR.PT
Application Container	A virtualization approach in which applications are isolated to a known set of dependencies, access methods, and interfaces.	PR.AC, PR.DS, PR.IP, PR.MA, PR.PT
Remote Desktop Access	Remote desktop access solutions provide a mechanism for connecting to, and controlling a remote computer, either physical or virtual.	PR.AC, PR.DS, PR.IP, PR.MA, PR.PT

Unified Communications and Collaboration

Telework often requires virtual meetings, frequently conducted using unified communications and collaboration (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 that have access to that content. To that end, UCC services must be selected that offer protections appropriate to the content to be shared. 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, HIPAA) while other versions lack those protections. Virtual meeting participants need to exercise caution and awareness of the content they are sharing to ensure that only authorized content is shared. Participants also need to be aware that any content shared may be shared more widely than they intended; other attendees may be using screen capture devices or otherwise recording any and all content, whether by microphones and/or cameras broadcasting undesired additional content or extraneous content when sharing screens. Particular care should be taken when sharing and receiving files, as well as when providing remote control to a computer, especially if left unattended.

Unified Communications and Collaboration Capabilities

Capability	Description	NIST CSF Mapping
UCC Identify 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.	PR.AC
UCC Encrypted Communication	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.	PR.PT, PR.DS

Capability	Description	NIST CSF Mapping
UCC Connection Termination	Mechanisms which ensure the meeting host can positively control participation. These can include inactivity timeouts, on-demand prompts, unique access codes for each meeting, host participant eviction, and even meeting duration limits.	PR.AC, PR.IP, PR.AT
UCC Data Loss Prevention	Mechanisms for controlling the sharing of information between UCC participants, intentional or incidental. This may be integrated into additional agency data loss prevention technologies and can include keyword matching, attachment file type or existence prohibitions, attachment size limitations, or even audio/visual filters.	PR.DS

Data Protection

Data protection is the process of maintaining the confidentiality, integrity and availability of an agency's data consistent with the agency's risk management strategy. It is important that agencies secure their data from corruption, compromise, or loss. The surge in telework requires agencies to 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-owned devices, as well as on remote devices that are not owned by an agency. Policies, procedures, user training, and incident response may require adaptations to accommodate new telework services and data handlining, storage, and uses.

Data Protection Capabilities

Capability	Description	NIST CSF Mapping
Access Control	Access Control technologies allow agencies to define policies concerning the allowable activities of users and entities to data and resources.	PR.AC, PR.IP, DE.CM
Protections for Data at Rest	Data protection at rest aims to secure data stored on any device or storage medium.	PR.DS
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.	PR.DS
Data Loss Prevention	Data Loss Prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	PR.DS
Data Access and Use Telemetry	Data access and telemetry identify agency sensitive data stored, processed, or transmitted, including those located at a CSP. Enforce detail logging for access or changes to sensitive data.	ID.AM, PR.AC, PR.DS, PR.PT, DE.AE, DE.CM

APPENDIX A: SERVICE PROVIDER OVERLAY

The tables below are intended for (1) vendors to align their products and services to TIC telework security capabilities described in the previous tables, and (2) for agencies to use the resulting overlays to identify products and services that fulfill TIC guidance in a way that meets their risk tolerance and business mission needs during the telework surge.

Definition of Table Fields

TIC Capability – Identifies the security capability from the TIC Security Capabilities List for Telework section of this document.

Vendor Service Name – Vendor assigned product(s) or service(s) intended for alignment with TIC security capabilities. This column contains two fields to identify one or more primary services that directly fulfill the capability and one or more complementary services that partially fulfill or support fulfillment of the capability. Vendors may include services that primarily fulfill capability requirements in the primary service column; vendors may also include services that provide enhancements to security in addition to their primary function in the complementary service column. Vendors may leave columns blank if no services fulfill a capability requirement.

1. Universal Security Capabilities

<Vendor/Service Name> Service Mapping for Universal Capabilities

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
Backup and Recovery		
Central Log Management with Analysis		
Configuration Management		
Incident Response Plan and Incident Handling		
Inventory		
Least Privilege		
Secure Administration		
Strong Authentication		
Time Synchronization		
Vulnerability Assessment		
Audit and Accounting		

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
Resilience		
Enterprise Threat Intelligence		
Situational Awareness		
Dynamic Threat Discovery		
Policy Enforcement Parity		
Effective Use of Shared Services		
Integrated Desktop, Mobile, and Remote Policies		

2. PEP Capabilities

<Vendor/Service Name> Service Mapping for Files

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
Anti-malware		

<Vendor/Service Name> Service Mapping for Email

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
Anti-phishing Protections		
Data Loss Prevention		
Encryption for Email Transmission		
Malicious URL Protections		
URL Click-Through Protection		
NCPS E^{3}A Email Protections		

<Vendor/Service Name> Service Mapping for Networking

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
Network Segmentation		
Microsegmentation		

<Vendor/Service Name> Service Mapping for DNS

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
DNS Blackholing		
DNSSEC for Agency Clients		
DNSSEC for Agency Domains		
NCPS E^{3}A DNS Protections		

<Vendor/Service Name> Service Mapping for Intrusion Detection

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
Adaptive Access Control		
Endpoint Detection and Response		

<Vendor/Service Name> Service Mapping for Intrusion Enterprise

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
VPN		
Application Container		
Remote Desktop Access		

<Vendor/Service Name> Service Mapping for Unified Communications

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
UCC Identify Verification		
UCC Encrypted Communication		
UCC Connection Termination		
UCC Data Loss Prevention		

<Vendor/Service Name> Service Mapping for Data Protection

TIC Capability	Name(s) of Primary Vendor Service(s)	Name(s) of Complementary Vendor Service(s)
Access Control		
Protections for Data at Rest		
Protections for Data in Transit		
Data Loss Prevention		
Data Access and Use Telemetry		