CAPACITY ENHANCEMENT GUIDE: REMOTE PATCH AND VULNERABILITY MANAGEMENT

PURPOSE

The purpose of this document is to assist federal agencies with patching roaming devices, i.e., remote devices outside agency campus networks. Traditional vulnerability and patch management solutions require that all roaming devices first establish a trusted connection to—and route all remote traffic back through—agency campus networks. However, when routing traffic through agency campus networks, agencies face challenges related to virtual private network (VPN) bandwidth constraints, which are impacting the timely patching of roaming devices and degrading or interrupting other vital services being accessed from roaming devices. These significant delays in patching leave roaming devices susceptible to common vulnerabilities and threats. Recent increases in teleworking have amplified these issues and made securing roaming devices even more challenging.

In April 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released Trusted Internet Connection (TIC) 3.0 Interim Telework Guidance, which provided an alternative solution for remote vulnerability and patch management, allowing agencies to route associated traffic directly to agency-sanctioned cloud service providers (CSPs), thus bypassing limited bandwidth connections back to agency campus networks.

This guide assists federal agencies in leveraging the TIC 3.0 Interim Telework Guidance to improve remote vulnerability management efforts to meet the growing demands on network capacity that may otherwise require an increase in bandwidth for existing internet service provider (ISP) or VPN services.

SCOPE

This guide applies to remote patch and vulnerability management for software (e.g., operating systems and applications) on managed end-user roaming government-furnished equipment (GFE) devices (e.g., laptops) running Microsoft Windows or MacOS operating systems. The guide does not apply to mobile devices (e.g., running Android or iOS), unmanaged GFE, and non-GFE devices (known as "bring your own device" or "BYOD").

For the purposes of this guide,

- A **roaming device** is a managed GFE endpoint (e.g., laptop) used by remote workers to access— traditionally via VPN—an agency's data and systems.
- An **agency-sanctioned cloud service** is a cloud service authorized by the Federal Risk and Authorization Management Program (FedRAMP) at a level commensurate with the categorization of target devices.
- An **agency-curated patch repository** is a centralized patch management technology that identifies and acquires patches and deploys these to—and verifies them on—agency devices. It can deploy software updates that include vendor-supplied and agency-verified code signing certificates and chain-of-trust certification paths that use Public Key Infrastructure technologies to confirm authenticity and validate each component from the end entity to the root certificate. This validation includes transactional integrity and verification leveraging session encryption validated by an agency-controlled trust center.

CONSTRAINTS AND ASSUMPTIONS

This guide:

- Leverages the TIC 3.0 Interim Telework Guidance for remote management of patches and vulnerabilities on roaming devices.
- Is valid for as long as the TIC 3.0 Interim Telework Guidance is in place or is integrated into the TIC 3.0 Remote User Use Case.
- Focuses on TIC 3.0 adaptations for communications between roaming devices and agency-sanctioned cloud services. Note: Roaming device communications with agency-campus-hosted resources and with web entities should continue to follow established agency protections.
- Is only intended to address scenarios in which agency roaming devices connect remotely to agency campus networks and agency-sanctioned cloud services hosting an agency-curated patch repository that follows the same policies as the on-premise patch management solution.

Any traffic to the public internet (e.g., traffic to public websites) must still be routed through EINSTEIN sensors, the operational capabilities of the National Cybersecurity Protection System program. When in doubt, agency traffic should be routed through EINSTEIN sensors.

RECOMMENDED SCENARIO

The traditional approach to vulnerability and patch management is agencies manage devices from a centralized platform hosted on campus networks, from which devices receive patches and updates. This approach works well with on-premise devices, but once these devices leave agency networks they must first establish a trusted connection to agency campus resources (e.g., VPN) and the vulnerability and patch management traffic must compete for limited bandwidth with other critical services. Aggregating all teleworker traffic through a single location facilitates security policy enforcement and protections at a central location, but it also may require additional resources, incur greater costs, and decrease network and service performance.

The TIC 3.0 Interim Telework Guidance allows a scenario that permits roaming devices to directly access resources in agency-sanctioned cloud environments while preserving policy enforcement and accommodating various risk tolerances. As shown in figure 1, the guidance allows limited and controlled routing of traffic directly from roaming devices to CSPs without a need to route it back through agency VPNs and traditional TICs. It clarifies the TIC split-tunneling options and allows for a specific patch management scenario that reduces the burden on agency VPNs and improves user experience.

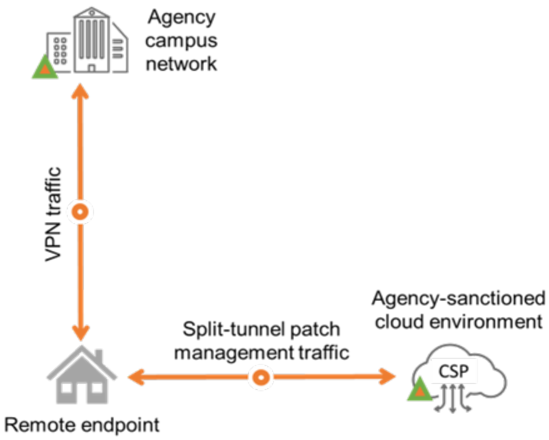
Agency campus network
VPN traffic
Agency-sanctioned cloud environment
Split-tunnel patch management traffic
CSP
Remote endpoint

Figure 1 TIC 3.0 Interim Telework Guidance

In this scenario agencies still centrally manage their endpoints, but the vulnerability and patch management platform is hosted in an agency-sanctioned cloud environment and allows roaming devices to use split tunneling to access cloud-based resources directly (or through a cloud access security broker [CASB] or another security as a service provider) without having to route the bandwidth-intensive patch-management traffic back to the agency campus network through VPN connections.

Agencies using this approach must ensure that remote device traffic destined for the cloud-based solution is properly constrained to sanctioned destinations and that roaming devices do not connect to unsanctioned resources, i.e., individual software applications are not allowed to directly access and download updates from vendor sites.

While vendors are encouraged to map their service offerings to the suggested TIC objectives and security capabilities, agencies still need to work with vendors to identify appropriate implementation approaches that align with agency risk tolerances. Agencies should discuss the availability of log and telemetry features to determine the relevant information they would need to provide to CISA for cybersecurity analytical purposes.

Roaming device split-tunnel traffic not routed back to agency campus networks must remain aligned with the TIC security capabilities as outlined in the TIC 3.0 Interim Telework Guidance. Agencies should maintain a policy for—and enforce—concurrent or mutually exclusive connectivity.

Agencies should document all resulting risk decisions and the agency's senior official responsible for risk management (or equivalent) should approve these in accordance with agency internal procedures.

This guide is intended to complement and does not supersede any recommendations made in the TIC 3.0 Interim Telework Guidance.

The following checklist summarizes requirements that must be met to allow for implementation of the cloud- based solution for remote vulnerability and patch management:

- ✓ The implementation approach is in alignment with agency risk tolerance, is properly documented, and is approved by the agency senior official responsible for risk management or equivalent.
- ✓ Roaming devices are agency owned (GFE).
- ✓ Roaming devices are centrally managed.
- ✓ Roaming devices are configured to disable receiving automatic updates for the operating system and individual software directly from vendors.
- ✓ Roaming devices are configured to receive updates from agency-authorized patch and vulnerability management solution.
- ✓ Roaming device traffic related to authorized vulnerability and patch management is constrained to an agency-sanctioned cloud solution only.
- ✓ Roaming device split-tunnel traffic not routed back to agency campus network is aligned with the TIC security capabilities as outlined in the TIC 3.0 Interim Telework Guidance and there is a policy in place—and enforcement for—concurrent or mutually exclusive connectivity.
- ✓ The cloud-based vulnerability and patch management platform is FedRAMP authorized at the level that is commensurate with the categorization of target devices.
- ✓ Agency-sanctioned cloud services host an agency-curated patch repository that follows the same policies as the on-premise patch management solution.

CONTACT INFO

For questions about this guide and other CISA services available to federal agencies, please contact CyberLiaison@cisa.dhs.gov.