TLP:CLEAR

JOINT CYBER DEFENSE COLLABORATIVE

JCDC
REMOTE MONITORING & MANAGEMENT
CYBER DEFENSE PLAN

AUGUST 2023

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)

The Cybersecurity & Infrastructure Security Agency (CISA) spearheads the national effort to defend against cyber threat actors that target U.S. critical infrastructure, federal and state, local, tribal, and territorial (SLTT) governments, the private sector, and the American people. While CISA serves a foundational and essential role in this effort, cybersecurity is a shared responsibility, and the Nation must work collectively to manage and reduce cyber risk. Close collaboration between government, industry, international, and other partners is needed to reduce the prevalence and impact of damaging intrusions today to achieve a more secure future.

THE JOINT CYBER DEFENSE COLLABORATIVE (JCDC)

In 2021, pursuant to new authority from Congress, CISA created a new kind of partnership—the Joint Cyber Defense Collaborative (JCDC)—to mature CISA's traditional public-private partnerships into real-time private-public operational collaboration with a focus on proactive planning and mitigation. JCDC combines the visibility, insight, and innovation of the private sector with the capabilities and authorities of the federal cyber ecosystem to enable partners to collectively drive down cyber risk to the Nation at scale. Through JCDC, CISA unifies and synchronizes the collective cyber defense of federal agencies, SLTT entities, international allies, private sector entities, and other partners.

THE 2023 JCDC PLANNING AGENDA

CISA and partners were proud to announce the JCDC's 2023 Planning Agenda in January 2023 to advance this critical aspect of our work. This agenda is a forward-looking effort that is bringing together government and the private sector to develop and execute cyber defense plans that achieve specific risk reduction goals and enable more focused collaboration. CISA will continue to expand the breadth and depth of this partnership to maximize both the completeness and impact of these planning efforts. Through a rigorous process that includes input from subject matter experts and government and private sector partners, CISA developed a Planning Agenda focused on three topic areas: systemic risk, collective cyber response, and high-risk communities. CISA is currently using this same process to develop the 2024 JCDC Planning Agenda.

REMOTE MONITORING & MANAGEMENT (RMM) PLANNING EFFORT

JCDC's 2023 Planning Agenda prioritizes the mitigation of systemic cybersecurity risks. In working with partners across government and the private sector, CISA identified that exploitation of RMM software presents a systemic risk to organizations across sectors. By exploiting RMM products, cyber threat actors can gain footholds into managed service provider (MSP) servers and, by extension, into thousands of small and medium-sized business (SMB) customer networks that employ MSPs. The use of RMM software or MSPs that use RMM software introduces an attack surface that can result in compromises, particularly affecting end-user organizations with limited cybersecurity expertise. Exploited vulnerabilities in RMM services can have cascading impacts across the globe and impact industries that collectively make up more than 40% of all private sector payroll in the United States. For instance, ransomware threat actors continue to use RMM tools in their attacks, presenting a growing risk to SMBs that support national critical functions. To reduce these types of risk at scale, JCDC convened key partners and authored the JCDC RMM Cyber Defense Plan, which sets forth a collective plan for cyber defense

REMOTE ADMINISTRATION SOLUTION:
Software that grants a remote entity remote access to an endpoint's applications and network access; This software can also grant unattended, possibly transparent, administrative control to a device remotely.

REMOTE MONITORING AND MANAGEMENT:
Software installed on an endpoint to continuously monitor a machine or system's health and status, as well as enabling remote unattended administration functions including unattended modification to the endpoint's security configuration, installed applications, and local accounts.

leaders in government and the private sector to mitigate threats to the RMM ecosystem. Through the 2023 planning effort, JCDC aims to build and leverage relationships with this strategic ecosystem of RMM vendors, MSPs, and MSSPs, to address a maturing and evolving threat to U.S. critical infrastructure by creating enduring partnerships centered on operational engagement, information sharing, and education across the cyber ecosystem.

TECHNOLOGY AND RISK ENVIRONMENT

According to a 2022 report, approximately 90% of U.S.-based small and medium-sized businesses (SMBs), to include critical infrastructure entities, rely on MSPs to supplement their own information technology (IT) , operational technology (OT) and industrial control systems (ICS) capabilities, and scale network environments without having to develop and manage these capabilities internally. Many MSPs and managed security service providers (MSSPs) in turn rely on RMM vendors for software deployment, account management, and other software tools. The structure of the RMM ecosystem (Figure 1) presents an opportunity to advance cybersecurity and reduce supply chain risk at scale for small and medium critical infrastructure entities.

RMM software allows IT service providers to remotely monitor and operate devices and systems, as well as attain heightened permissions, enabling MSPs or IT help desks to monitor multiple devices and networks simultaneously. These capabilities can be exploited by malicious cyber actors who leverage them to establish network connections through cloud-hosted infrastructure while evading detection. These types of intrusions are also known as living off the land (LOTL) attacks, where adversaries no longer have to rely on inherently malicious files, codes, and scripts, and instead use tools already present in the environment to enable their malicious activity. This form of intrusion makes businesses even more vulnerable to service provider supply chain compromises, exploitation, or malicious use of remote capabilities.

The CISA product Guide to Securing Remote Access Software, released on June 6, 2023 as part of this Cyber Defense Plan, identifies how remote access software is particularly appealing to threat actors because the software:

- Does not always trigger security tools,
- does not require extensive capabilities development,
- may allow actors to bypass software management control policies,
- could allow actors to bypass firewall rules, and
- can facilitate multiple cyber intrusions.

Reflecting the risk LOTL attacks pose to U.S. critical infrastructure, CISA released a recent joint Cybersecurity Advisory (CSA) that provides insight on how a People's Republic of China (PRC) state-sponsored cyber actor, also known as Volt Typhoon, is leveraging LOTL attacks as one of its primary tactics, techniques, and procedures (TTPs). Private sector partners have identified that this activity affects networks across U.S. critical infrastructure sectors, and the authoring agencies believe the actor could apply the same techniques against these and other sectors worldwide.

MANAGED SERVICE PROVIDER (MSP): A business entity who, in whole or in part, provides IT related services or application management for another organization.

MANAGED SECURITY SERVICE PROVIDER (MSSP): A business entity who solely provides information security services and applications to another organization.

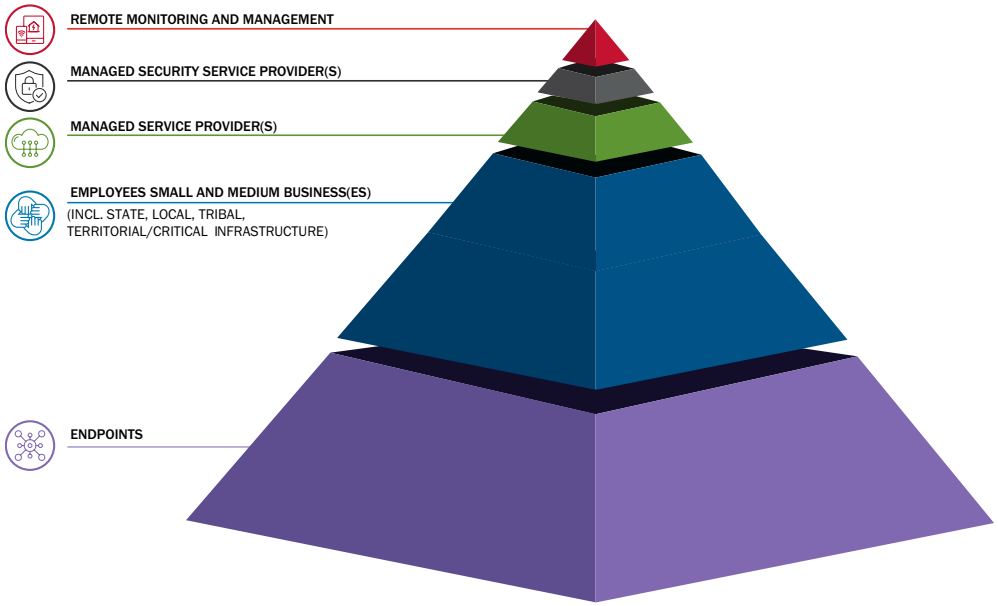

FIGURE 1: *RMM Ecosystem*

JCDC RMM CYBER DEFENSE PLAN OVERVIEW

The *JCDC RMM Cyber Defense Plan* aligns with the priorities outlined in the *CISA Strategic Plan 2023–2025* and highlights specific lines of effort addressed in the *National Cyber Strategy 2023.* Per the *National Cybersecurity Strategy*, JCDC has a responsibility to integrate cyber defense planning and operations across the Federal Government and with the private sector. To support the *CISA Strategic Plan,* the *JCDC RMM Cyber Defense Plan* identifies a path forward to reduce risks to—and strengthen the resilience of—America's critical infrastructure organizations that are dependent upon RMM products.

The *JCDC RMM Cyber Defense Plan* was developed by a core planning team, led by the JCDC Planning Office, and included representation from other divisions across CISA, the Federal interagency, and private industry. The components of the *JCDC RMM Cyber Defense Plan* provide leaders in the RMM ecosystem with necessary ways and means for sustained, effective cyber defense at scale (as identified in Figure 2 and Table 1).

Central to the *JCDC RMM Cyber Defense Plan* is an operational community founded on trust and collaboration to drive joint cyber defense operations. This community ultimately aims to reduce the frequency and impact of cybersecurity incidents across the RMM ecosystem and leverage the prevalence of RMM software across critical infrastructure to scale cyber defense operations. JCDC places a heavy emphasis on fostering this culture of cooperation and looks to indicators like the number of actively participating organizations, the volume and quality of information shared, and the development and subsequent adoption of shared information, as measures of success and indication of a growing recognition of threats, cybersecurity challenges, and opportunities in this space.

> We must build new and innovative capabilities that allow the owners and operators of critical infrastructure, federal agencies, product vendors and service providers, and other stakeholders to effectively collaborate with each other at speed and scale.
>
> **National Cybersecurity Strategy, March 2023**

VISION A secure and hardened RMM ecosystem.

MISSION JCDC's RMM Cyber Defense Plan provides cyber defense leaders in government and industry with a collaborative proposal for mitigating threats to the RMM ecosystem.

GOALS

1. Understand how RMM vendors can help improve cybersecurity at scale and across critical infrastructure sectors.
2. Identify mechanisms to sustain cybersecurity collaboration between USG stakeholders and RMM vendors into the future.

PILLAR 1

OPERATIONAL COLLABORATION

"Establish enduring capabilities for persistent collaboration in which participants continuously exchange, enrich, and act on cybersecurity information with the necessary agility to stay ahead of our adversaries."

LOE 1: Cyber Threat and Vulnerability Information Sharing

LOE 2: Enduring RMM Operational Community

PILLAR 2

END-USER EDUCATION

"Joint enrichment and development of timely cybersecurity advisories and alerts to benefit the broader community."

LOE 3: End-User Education

LOE 4: Amplification

FIGURE 2: *JCDC RMM Cyber Defense Plan Vision, Mission, and Goals*

PILLAR 1: OPERATIONAL COLLABORATION

Effective partnerships and collaboration between the government and private sector are the foundation of our collective effort to protect the nation's critical infrastructure. Major RMM vendors have highlighted their willingness and desire to work with the USG; however, available partnerships or forums for sustained collaboration may not always be available or leveraged. JCDC aims to drive collective action across the RMM community to enhance information sharing, increase visibility, and fuel creative cybersecurity solutions.

LOE 1: CYBER THREAT AND VULNERABILITY INFORMATION SHARING

Expanding the sharing of cyber threat and vulnerability information between USG and RMM ecosystem stakeholders to increase reach speed, and effectiveness of RMM cybersecurity.

LOE 2: ENDURING RMM OPERATIONAL COMMUNITY

Institutionalize mechanisms that promote and facilitate long-term communication and collaboration amongst the RMM ecosystem stakeholders to continue scaled security efforts after the formal JCDC RMM planning effort has concluded.

PILLAR 2: CYBER DEFENSE GUIDANCE

At the base of the RMM ecosystem, SMBs account for 6.5 million business and over 40% of U.S. gross domestic product (GDP). Although CISA will continue to implement "top-down" initiatives, i.e. RMM stakeholder engagement, it is imperative to improve "bottom-up" visibility of CISA resources and guidance at the end-user level. According to a 2021 U.S. Telecom cyber survey, only 13% of small and medium-sized critical infrastructures entities are aware of and/or follow CISA guidance. To improve cybersecurity in the RMM ecosystem at scale, CISA must address fundamental gaps in target audience awareness. This pillar focuses on educating RMM end-user of the dangers and risk to their RMM infrastructure today, and how they can help promote security best practices moving forward.

LOE 3: END-USER EDUCATION

CISA, Interagency partners, and other RMM ecosystem stakeholders will work together to develop and enhance cybersecurity guidance to RMM end-users.

LOE 4: AMPLIFICATION

Currently CISA publishes certain products, such as advisories and/or alerts on its website for public consumption, to include by critical infrastructure operators of the RMM community. RMM ecosystem stakeholders use a combination of conventional and novel lines of communication to share information. The goal of amplification is to leverage all available lines of communication within the RMM ecosystem to amplify high-fidelity CISA advisories and alerts.

FIGURE 3: *JCDC RMM Cyber Defense Plan Lines of Effort (LOEs)*

ACCOMPLISHMENTS TO DATE

JCDC has already capitalized on the momentum of collaboration established through this planning effort and have advanced protections through this unique and strategic partnership. The enduring partnership provides a proven forum to drive industry-informed objectives aimed at mitigating risk to downstream SMBs and critical infrastructure operators. The actions below highlight efforts achieved to date.

- **EXPANDING THE PARTNERSHIP.** JCDC has expanded participation in operational collaboration fora to include strategic partners from across the RMM ecosystem. Through this relationship, RMM stakeholders will be able to maintain access to JCDC partner coordination channels that support real time information sharing, routinize coordination efforts in advance of and response to cyber incidents, and optimize communication. Likewise, through this new strategic partnership, RMM stakeholders are providing new avenues to amplify CISA services, cybersecurity guidance, and vulnerability and threat information across the RMM ecosystem, including to downstream SMBs and critical infrastructure operators.
- **WHOLE-OF-NATION CYBER DEFENSE PLANNING EFFORTS.** No single entity has the complete knowledge, capabilities, and legal authorities to defend the entire digital ecosystem against advanced persistent threat actors. Through this Cyber Defense Plan, RMM stakeholders were able to identify and develop future planning topics to help strengthen the cybersecurity posture of RMM end user organizations. JCDC will leverage momentum with this strategic operational community to identify priority areas for addressing systemic risk across the RMM ecosystem and to develop well-informed and impactful cyber defense plans to combat those significant systemic cyber risks and malicious actors. The ability to continue to expand and leverage the expertise of this strategic operational community will have positive downstream effects within the RMM ecosystem.
- **USING CYBERSECURITY SERVICES.** Through this planning effort RMM stakeholders have been introduced to the full suite of CISA cybersecurity services. RMM stakeholders will continue to have access to CISA's services that can help identify vulnerabilities they can remediate before a cyber threat actor has the chance to exploit them, including participation in CISA Ransomware Vulnerability Warning Pilot and Pre-Ransomware Notification Initiative. This partnership will create the opportunity for RMM stakeholders and CISA to coordinate more closely to identify and implement security improvements that will improve the security posture of the overall RMM ecosystem, from RMM vendors to SMBs and critical infrastructure operators.
- **PRODUCTS AND COMMUNICATION.** In partnership with RMM stakeholders, CISA will continue to provide guidance to help organizations address the risk of adversary targeting across the RMM ecosystem. Most recently, CISA released the following two resources to help defend against RMM targeting.
    - *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,* released on May 24, 2023. This advisory highlights how a PRC cyber actor is living off the land using built-in network administration tools to evade detection while compromising networks and conducting malicious activity. This tactic enables the actor to evade detection by blending in with normal Windows system and network activities, avoid endpoint detection and response (EDR) products, and limit the amount of activity that is captured in default logging configurations. This advisory will help organization's network defenders hunt for this activity on their systems. It provides many network and host artifacts associated with the activity occurring after the network has been initially compromised, with a focus on command lines used by the cyber actor.
    - *Guide to Securing Remote Access Software*, which provides an overview of common exploitations and associated tactics, techniques, and procedures. It also includes recommendations to IT/OT and ICS professionals and organizations on best practices for using remote capabilities and how to detect and defend against malicious actors abusing this software.
- **ADVANCING SECURE BY DESIGN/DEFAULT**. CISA is focused on the development of secure by design/default into all information technology products. Through this planning effort, RMM stakeholders identified that they have an important role to play alongside the government in driving to improve security by design across their products. RMM stakeholders along with CISA will continue to work closely to identifying secure by design/default RMM principles to strengthen the RMM ecosystem.

CONCLUSION

The ubiquity of RMM software, coupled with the sizable market share of several key RMM stakeholders, positions JCDC to facilitate systemic positive impacts across the cyber domain. Enhancing the cyber resilience and threat awareness of RMM stakeholders can provide downstream benefit to end-users, including SMB owners and critical infrastructure operators. The JCDC RMM Cyber Defense Plan presents a foundation from which leaders across CISA, Interagency partners, and industry partners can suitably align and delineate their respective lines of effort to accomplish key objectives. JCDC will continue to lead the execution of the JCDC RMM Cyber Defense Plan, relying on external stakeholders both within and outside of CISA. Public-private collaboration in the RMM ecosystem is, and will remain, a vital component of CISA's mission to understand, manage, and reduce risk to our nation's critical infrastructure.

DISCLAIMER

CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

ACKNOWLEDGEMENTS

ANB Bank, CompTIA, ConnectWise, CNWR, Corporate Information Technologies, CyberRX, Department of the Treasury, Huntress, ISC2, Kaseya, N-Able, and The Open Group contributed to this cyber defense plan.