CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

NETWORK SECURITY MANAGEMENT – What is Happening on the Network? How is the Network Protected?

OVERVIEW OF NETWORK SECURITY MANAGEMENT

The Cybersecurity and Infrastructure Security Agency's Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security postures. The CDM Program ultimately reduces the threat surface and improves federal cybersecurity response through four capability areas: Asset Management, Identity and Access Management, Network Security Management (NSM), and Data Protection Management.

The NSM capability is designed to provide agencies with greater visibility into what is happening on their networks, which also gives them a better understanding of how the networks are being protected. This capability makes use of defense-in-depth boundary protection mechanisms and incident detection and response procedures to protect agencies against hacking, misuse, and unauthorized changes of network devices. NSM capabilities protect the external and internal boundaries of agency systems by providing visibility into network behavior, firewall traffic, encrypted and decrypted data, virtual private network connection, and ports and protocols. NSM consists of four overarching component capabilities, including: boundary protection (BOUND); manage events (MNGEVT); operate, monitor, and improve (OMI); and design and build in security (DBS).

BENEFITS OF NETWORK SECURITY MANAGEMENT

NSM includes network and perimeter components, host and device components, cryptography management, and security event management (e.g., user behavior, device logging). This capability allows agencies to develop timely incident-response procedures, identify potential threat vectors, and reduce their attack surface by implementing risk management techniques. NSM also supplies agencies with the tools necessary to prepare for and respond to incidents, ensure that software and system quality is integrated into network infrastructure, and prevent adversarial pivoting throughout the network.

NETWORK SECURITY MANAGEMENT CAPABILITIES

NSM is comprised of four component capabilities and three sub capabilities to help agencies gain visibility into what is happening on their networks.

Boundary protection

BOUND limits, prevents, and/or allows the removal of unauthorized network connections. This capability is responsible for monitoring and controlling borders and protection mechanisms for an agency network by detecting and deterring malicious activity. BOUND is categorized into three security capabilities:

- **Filters and boundary controls (BOUND-F)**
  BOUND-F manages network filters and controls through firewalls and gateways that sit at the boundary separating the internal network from the external network. These filters regulate the flow of traffic between the trusted and less-trusted sides of the network. BOUND-F focuses on network weaknesses and vulnerabilities that can affect the network's ability to prevent the disclosure of confidential data, determine when the integrity of the network is compromised, and detect when malicious behavior impacts the network's availability.

- **Network access control (NAC)**
  NAC ensures that a device can connect to an agency network only if the device is compliant with the agency's hardware and software configuration and patching policies, thereby reducing the network attack surface. This capability provides agencies with a reliable and effective way to protect their network from unauthorized access by utilizing modern tools such as logging and alerting systems, access control systems, Policy Enforcement Points (PEPs), and more.

- **Monitor and manage cryptographic mechanisms controls (BOUND-E)**
  BOUND-E provides visibility into risks associated with the use of cryptographic mechanisms deployed on an organization's network. This capability enables agencies to identify improper cryptographic behavior on the network, ensuring encryption is properly implemented and configured to provide the desired level of protection. BOUND-E uses cryptography techniques and key management/Certificate Authorities (CA) to ensure communication and sensitive information is properly encrypted and secured.

Manage events

MNGEVT identifies security threat vectors by utilizing security event information from multiple sources within an agency network. This facilitates proactive and timely detection of intruders and security risks, both internal and external to the organization. MNGEVT establishes processes and procedures for incident response, privacy, contingency planning, audit and accountability, and ongoing assessment to strengthen an agency's security posture.

Operate, monitor, and improve

OMI focuses on in-depth analysis of security events, prioritization of security mitigation response and recovery, notification of events, and reporting of post-incident activity. This capability dynamically monitors the security risk level using results from the MNGEVT ongoing assessments to detect when changing threats, vulnerabilities, technologies, and mission/business process may result in an unacceptable risk level.

Design and build in security

DBS ensures security features are incorporated into all stages of the software development lifecycle. This capability combines with supply chain risk management concepts to reduce the attack surface for network and infrastructure components. DBS focuses on designing components that will be used for the software or device, developing and testing information system components to ensure that their security and privacy needs are implemented effectively, verifying security and privacy requirements have been met, and ensuring that security goals are established and monitored.

CURRENT STATE OF CDM NETWORK SECURITY MANAGEMENT DEPLOYMENT

Multiple components of NSM have been deployed within agencies, such as incident-response reporting, BOUND, and cloud services. The CDM Program continues to work with agencies and industry partners to identify and prioritize the deployment of the NSM capability. Ultimately, NSM data will be reported to the CDM Agency Dashboard (which enables agencies to see their most critical cyber risks) and the Federal Dashboard (which provides summary information about cybersecurity risks across the Federal Government).

For more information on NSM capabilities and/or the CDM Program, please contact the CDM Program Management Office at CDM@cisa.dhs.gov.