FORESCOUT

INABILITY TO ACCOUNT FOR NETWORKED ASSETS WILL HINDER DEFENSE CONTRACTORS' ACHIEVEMENT OF CMMC

April 3, 2020

By Dean Hullings

Global Defense Solutions Strategist

Forescout is actively engaged with the defense contractor community to implement Cybersecurity Maturity Model Certification (CMMC) controls. Forescout's core capabilities that are of particular interest to defense contractors considering the CMMC include: identifying and assessing devices on networks, controlling access to and within the network and addressing many found vulnerabilities—whether by directly remediating, initiating remediation actions or quarantining devices. In Forescout's experience, most

defense contractors lack awareness of approximately fifty percent of the connected devices on their networks before they deploy the Forescout platform. Undetected and unmanaged assets represent both a dangerous threat surface and a significant obstacle to providing accurate reporting to the U.S. Department of Defense (DoD) under the new CMMC requirements.

What is CMMC?

In January 2019, the DoD published CMMC Version 1.0, a new set of cybersecurity standards that contractors handling various forms of Covered Defense Information, including Controlled Unclassified Information, must meet. This essentially captures all companies that conduct business with the Department of Defense.

Requirements for contractors to meet specified levels of the CMMC will be included in certain Requests for Proposals beginning in June 2020, and on a broader basis, in the fall of 2020. Also, CMMC will be a part of all new DoD contracts by 2026.[1] The major difference between CMMC and the standard it replaces (NIST Special Publication (SP) 800-171, commonly referred to as "DFARS") is that CMMC provides a robust enforcement process: compliance with CMMC will be subject to audit by third-party assessors.

To be eligible for DoD contract award, suppliers will be required to institute both "practices" (i.e. controls) and "processes" that correspond to a specified maturity level between one and five (five being most mature). Encapsulated in the CMMC are 171 practices that enable 43 capabilities which are assigned to a security domain, of which there are 17. Process maturity essentially measures the degree to which security practices are institutionalized. Maturity levels for both are cumulative; for example, achieving level four requires meeting levels 1-3.

How does CMMC differ from previous requirements?

Current DoD suppliers are likely familiar with the bulk of CMMC practices, since the majority of them, specifically 110 of the 171 practices, originate from FAR Clause 52.204-21[3] and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 per DFARS clause 252-204.7012[5]. Other requirements come from reputable sources such as NIST SP 800-53, NIST Cybersecurity Framework, CERT Resilience Management Model and Center for Internet Security (CIS) controls.

Unlike NIST SP 800-171, however, compliance with the CMMC will be verified by accredited third-party assessors to determine whether a DoD supplier/contractor has met the maturity level required to perform the DoD contract. In effect, compliance with SP 800-171 only required DoD suppliers/contractors to declare that they had developed (or were developing) System Security Plans and Plans of Action and Milestones. Under CMMC, the inability to achieve required maturity levels will disqualify companies from a DoD contract award.

Many aspects of the certification process remain undetermined, even as the CMMC requirements are being finalized. What is known now is that the CMMC Accreditation Body [2] will license assessors to certify DoD contractors. Third-party assessors have not yet been named, but over 200 organizations have indicated interest in becoming CMMC auditors,[3] and registration for being designated as such is likely to occur in the second quarter of 2020. [4]

Robust asset detection and inventory capabilities elude most organizations

Since CMMC was announced in July of 2019, Forescout has performed approximately three dozen cybersecurity assessments for medium and large defense companies looking to better prepare for CMMC. Forescout found that all contractors had numerous instances of devices on their networks that they previously did not know existed. Additionally, the Forescout platform discovered unknown software applications, almost all of which had known and unaddressed vulnerabilities. Forescout also found evidence of particular challenges that may be unique to the defense sector; for example, the persistence of Kaspersky applications at higher rates than Forescout typically finds within its commercial customer base. This finding is consistent with the assumption that defense contractors represent an attractive target for nation-state actors.

Here are anonymized findings of a cybersecurity assessment for one defense contractor:

Instances of unknown hardware applications:

- 2 smart speaker devices placed in sensitive locations
- 5 unknown or previously unidentified wireless devices and wireless access points that were added to the network to provide easier access or improved signal strength

- Several devices identified on the corporate network that were supposed to be connected to a less secure building systems network (devices were being accessed remotely by contractors)

Instances of unknown software applications:

- 27 instances of Kaspersky and Kaspersky-furnished files (e.g. embedded)

Instances of known but high-risk software applications or associated code:

- 12+ instances of endpoints running legacy unpatched Windows operating systems versions
- Dozens of instances of previously unknown software applications, nearly 100 percent of which contained known and unaddressed vulnerabilities
- Dozens of instances of known but unpatched versions of various software applications, with up to 50 percent containing known vulnerabilities

Other policy violations:

- The existence of a rogue network segment established to allow for remote employee access
- Two examples of networks believed to be air-gapped, but shown by Forescout to be accessible remotely (enabled by accident/poor design)
- Instances of endpoints that were dual-homed, in violation of policy (including one in which an employee installed a second network interface card on a Windows machine to bypass a slow VPN)

How Forescout helps defense customers comply with CMMC

Forescout products directly or indirectly address most of CMMC's requirements, from the visibility of networks and control of network access to visibility and control of endpoints themselves. Many of these requirements are similar to and overlap with the requirements the DoD must itself follow under the Comply-to-Connect program, for which Forescout provides several foundational capabilities.

The Forescout platform allows organizations to continuously detect, profile, determine the necessary authorization, evaluate the security posture of, and enforce policy-based controls on all connected devices, including non-traditional operational technology (OT) such as building automation systems and industrial controllers. Forescout also allows organizations to monitor and analyze communications between specific devices or groups of devices, offering a comprehensive understanding of device behavior, and the ability to enforce policies across all network environments (campus, cloud, data center and VPN/remote networks). Forescout assesses device compliance against an organization's security standards and can itself take steps or can activate other security and management tools in the environment, to remediate found problems.

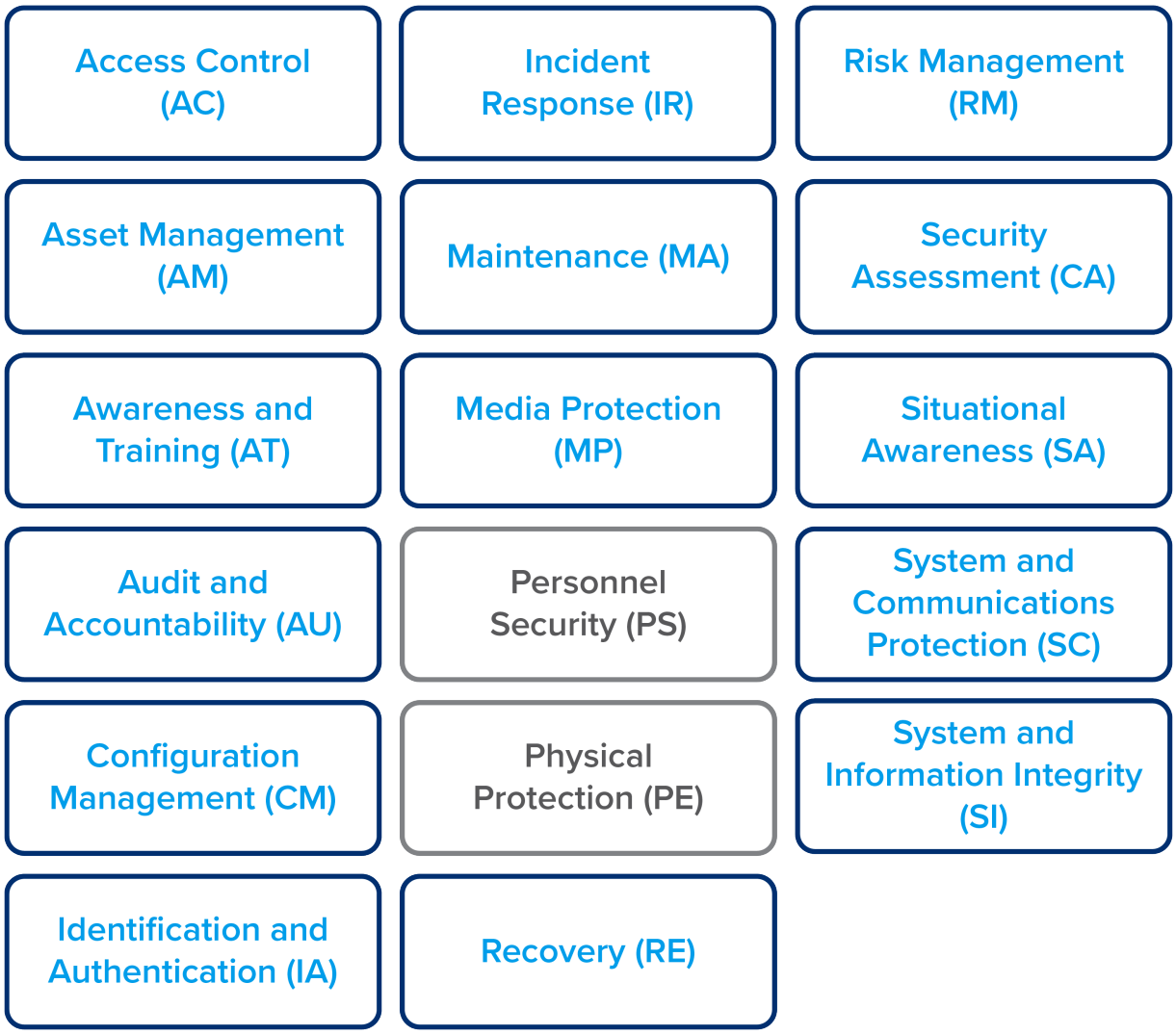
Forescout's Unrivaled Asset Detection Capability is the Standard Across the U.S. Federal Government

The Forescout platform does not require security agents on endpoints, and therefore allows organizations to detect and profile every single asset connected to their networks across all network environments (campus, cloud, data center, and VPN/remote networks). The U.S. Federal Government has selected Forescout's solution as its single source of truth for hardware asset discovery and inventory as part of two government-wide cybersecurity programs: Continuous Diagnostics and Mitigation and Comply to Connect. Using the Forescout platform, federal civilian agencies discovered, on average, 75 percent more assets on their networks than were previously known. In some cases, this figure was 200 percent.[1] Forescout's asset detection capabilities extend to hardware and software.

How Forescout supports achievement of CMMC

- Transactional policy-based **Access Control**
- User/Device **Identification and Authentication**
- Quick **Recovery** to "known good configuration"
- Feed **Asset Management** tool with accurate data
- Accurate log data for **Incident Response**
- Assess device compliance to quantify **Risk**

- Make user **Aware** when device is non-compliant
- Focus scarce resources on **Maintenance**> priorities
- Policy-based **Security Assessment** defined by user role and/or device category
- Accurate asset inventory for **Audit** accuracy
- Detect/block unauthorized digital **Media**
- Real-time compliance **Situational Awareness**
- Ensure proper **Configuration** of devices
- Segment **System to Protect against malicious code effects spreading across network**
- **Automated remediation for System Integrity**



As illustrated in the graphic above, asset visibility—including identification and authentication as well as security assessment—is the foundation for effective risk assessment and automated isolation and remediation of at-risk endpoints. This level of domain awareness can help prevent cyber incidents as well as facilitate response to and recovery from them. It enables systems administrators and corporate leadership alike to oversee response activities and restore systems and endpoints to a known configuration that meets security compliance standards in an effective and efficient manner.

Defense contractors must also remove banned products

Separate from the CMMC requirements, section 889(a)(1)(B) of the Fiscal 2019 National Defense Authorization (commonly referred to as “Part B”) directs that **no federal agencies may contract with any entity that uses products by Huawei, Zhongxing**

Telecommunications Equipment (ZTE) Corporation, Hikvision, Dahua Technology and Hytera. Contractors that have not deployed robust, machine-based asset detection capabilities will have difficulty finding all instances of these banned products and may, therefore, find it challenging to comply with Part B of section 889. Contractors that rely on procurement records to determine instances of banned products are unlikely to be truly compliant with the section 889 removal order. Federal agencies use Forescout's solution to comply with the same product bans, which easily determines the instances and locations of prohibited products to facilitate removal.

Contractors should concern themselves with OT sooner rather than later

Whether CMMC pertains to operational technology and Internet of Things (IoT) devices present on contractor networks remains a yet-unanswered question. The definition of "system" and "system assets" included in the CMMC controls specifically includes "specialized systems such as industrial/process control systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems."[5] The controls also call out Voice Over Internet Protocol (VoIP) phones and removable media. Yet DoD officials have not been clear on whether such devices and systems are in scope for the purposes of CMMC certification. Forescout strongly advises contractors to consider OT and IoT device detection and compliance now, as these devices' numbers are expanding rapidly and significantly in all organizations' networks, thereby increasing these organizations' threat surfaces. Forescout typically finds that organizations underestimate the amount of OT and IoT devices present on their networks by 25-35 percent. In addition, organizations often misidentify the OT and IoT devices they are aware of, and do not enforce basic segmentation or other policies or controls on them. Compounding the problem, these devices commonly lack even rudimentary security features and are often pre-set with easily-exploited security configurations. Forescout recommends that defense contractors deploy new technologies that can address OT and IoT devices—even if these devices are not explicitly within the scope of the CMMC.

Conclusion

The CMMC marks a dramatic shift away from DoD's previous requirements for ensuring strong cybersecurity practices from its suppliers. As CMMC rolls out, defense contractors and DoD officials alike should ask themselves a critical question: Can defense contractors who do not have a robust asset detection capability be truly confident that their reporting to the DoD is accurate? The device visibility, intelligence and control that Forescout provides is foundational to the DoD's own C2C program and can be instrumental to defense contractors' achievement of CMMC requirements.

[1] Jared Serbu, Pentagon issues long-awaited cyber framework for Defense industry, January 31, 2020.

[2] https://www.cmmcab.org/

[3] Complyup, CMMC Auditor Marketplace.

[4] https://www.cmmcab.org/c3pao

[5] https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf