THUNDERCAT TECHNOLOGY

A Service-Disabled Veteran-Owned Small Business

TANIUM

Preparing Higher Education Research Institutions for CMMC

ThunderCat Technology is a Service-Disabled Veteran Owned Small Business that delivers technology services and solutions to government organizations, educational institutions, and commercial companies. ThunderCat brings an innovative approach to solving customer problems in and around the datacenter.

Organizations that handle controlled unclassified information (CUI) and controlled sensitive information (CSI) – including many higher education research institutions – face constant threats from malicious actors. For example, in 2018, the Department of Justice charged nine Iranian hackers with stealing more than 31 terabytes of information from more than 300 higher education institutions. Reports found the total value of intellectual property stolen amounted to more than $3 billion.

The Department of Defense is mandating that these institutions, including University Affiliated Research Centers (UARCs) and Federally Funded Research and Development Centers (FFRDCs) who receive government grants to conduct research (and handle CUI/CSI) will soon need to meet the DoD Cybersecurity Maturity Model Certification (CMMC) alongside the Federal contractor community. The new guidelines are expected to go into effect in the fall of 2020.

A trained, accredited third-party organization called a Controlled Third Party Assessment Organization (C3PAO) will audit each contractor or research institution, validating compliance against a series of cybersecurity requirements and best practices, and assigning a cybersecurity maturity level for the organization.

How CMMC evaluates cyber maturity

The CMMC model measures cybersecurity against five levels. Each level includes a set of processes and practices, ranging from "performed" at Level 1 to "optimized" at Level 5. Each organization will be required to not only demonstrate the institutionalization of the practice, but also the implementation of all practices required for a specified level and all preceding levels, on an ongoing basis.

The auditing process takes a number of other factors into account, including the type and sensitivity of information handled, threats and implementation complexity.

Despite the model's name, this is not a check-the-box compliance exercise. The process provides a way to improve the alignment of cybersecurity practices with the type and sensitivity of information and associated threats.

The CMMC challenge for higher education

Historically, many FFDRCs and UARCs have had no centralized controls and were responsible for implementing, monitoring, and certifying their own IT systems security and any DoD CUI/CSI stored within those systems.

Today, to comply with CMMC guidelines, many of these institutions will need to turn to their central IT teams or third-party companies to create the IT infrastructure needed to meet CMMC standards and protect sensitive information from malicious actors.

Many lack the needed basic cyber hygiene processes, and most do not have the needed visibility into their full network – as we know, we can't control what we can't see. The team needs complete, continuous visibility into all assets on the network (an increasingly complex goal in the Internet of Things (IoT)/Bring-Your-Own-Device (BYOD) world).

Unfortunately, higher education institutions have created the final roadblock with the best of intentions. As they've worked to address individual cybersecurity vulnerabilities, most have implemented a complex patchwork of point products that don't integrate, are difficult to manage and keep patched, and can't give the IT leadership team a full view of the threats. Complexity equals risk plus cost. If institutions continue to implement a new/different point product to resolve individual problems, they will increase complexity, cost and risk. And, they won't achieve the visibility needed to manage risk and meet CMMC requirements.

Region 4 ESC Cyber Security Contract

Contract Number: R200804

http://www.thundercattech.com/contract-vehicles/omniapartners/

THUNDERCAT TECHNOLOGY

A Service-Disabled Veteran-Owned Small Business

TANIUM™

How Tanium helps with CMMC compliance

Higher education institutions need the capability to track and report network security status in near real-time, in line with CMMC requirements. Tanium helps unify and not just identify risks and vulnerabilities, but also prioritize them across the environment, and take action to respond and remediate in near real-time.

Tanium executes near instant queries of the environment, including millions of endpoints at one time, and creates near real-time reporting dashboards. This delivers speed and visibility, so you can fix issues, make changes quickly, and reduce risk. Tanium also enables continuous monitoring for compliance against the established benchmarks, likewise reducing risk.

CMMC compliance is one of the many things that keeps CISOs up at night. In the case of research universities, failure to meet the CMMC requirements could put DoD grant funding at risk. With Tanium's Unified Endpoint Management and Unified Endpoint Security solutions, however, CISOs have one less thing to worry about.

These solutions help reduce complexity, improve efficiency, and close the gaps between operations and security teams and provide CISOs a single platform to understand their environment and prepare them for future CMMC audits.

Tanium is not a C3PAO assessor – but we provide customers with high-fidelity insight into the cyber hygiene required for CMMC compliance. A few examples of assessment areas include:

Asset Discovery and Reporting

Tanium provides robust asset discovery and reporting. With the rise of the IoT and BYOD, there is the risk of (many) unknown devices on the network. When we run our discovery and asset tools in an organization's environment, we often identify an additional 12 to 20 percent of unknown devices.

Comprehensive Threat Monitoring

Tanium's unified endpoint management and security provides comprehensive threat monitoring with detailed incident analysis through a single platform to help identify, isolate and mitigate threats – and validate when they have been remediated.

Importantly, as Tanium completes nearly instant queries of the institution's environment, evaluating and analyzing millions of endpoints at one time, and pulls information into compliance reporting dashboards, the university has the best chance of preventing the loss of high-value intellectual property and CUI/CSI.

Visibility, control & compliance: Preparing for CMMC

While the auditing process is still being defined, C3PAO auditors will likely begin evaluations at high-profile research institutions widely known to conduct research that results in CUI or CSI.

Tanium can provide a path forward as these institutions address cyber hygiene and stand up a CMMC-compliant IT infrastructure.

While evaluating your institution's CMMC audit preparedness, start by considering the following questions:

- How many computers do you have on your network? And are they authorized to be there?
- What applications are installed? And are they all up to date?
- What are users doing? And is it authorized?
- How comfortable are you with your patch/vulnerability/risk posture?
- Have you recently been breached or had an outage that could have been prevented?

CMMC certification is critical for higher education research institutions to continue groundbreaking research. A healthy central IT infrastructure is essential to both protecting sensitive research data and identifying, preventing, and mitigating cyber risks.

About Key Partner: Tanium

Father and son founders David and Orion Hindawi make it their mission to empower the world's largest organizations to manage and protect their mission-critical networks. This singular focus led to the creation of the Tanium platform, which solves the biggest security and IT management challenges organizations face by providing lightning-fast ability to see everything and do anything across computer networks – with unparalleled scale.

TANIUM™

Region 4 ESC Cyber Security Contract

Contract Number: R200804

http://www.thundercattech.com/contract-vehicles/omniapartners/

THUNDERCAT TECHNOLOGY

A Service-Disabled Veteran Owned Small Business

THUNDERCAT TECHNOLOGY

OMNIA® PARTNERS

Tanium Receives 15% from the Omnia Cyber Contract OEMs Discount

15%

Link to Region 4 ESC Cyber Security Contract Pricing:

https://public.omniapartners.com/fileadmin/public-sector/suppliers/T-Z/ThunderCat_Technology/Contract_Documents/R200804/R200804_ThunderCat_PRC.pdf

Link to ThunderCat OMNIA Microsite:

https://www.thundercattech.com/contract-vehicles/omniapartners/

Link to ThunderCat OMNIA Microsite:

https://public.omniapartners.com/suppliers/thundercat-technology/contract-documentation

Other Resources:

ThunderCat Technology: https://www.thundercattech.com/
OMNIA Partners: https://www.omniapartners.com/
Tanium: https://www.tanium.com/

THUNDERCAT TECHNOLOGY

TANIUM™

Region 4 ESC Cyber Security Contract

Contract Number: R200804

http://www.thundercattech.com/contract-vehicles/omniapartners/