All Things Financial Management
Episode 10: Cybersecurity Capabilities of the Department of Defense with Mark Hakun

INTRO: Welcome to "All Things Financial Management," an ASMC podcast sponsored by Guidehouse, where we discuss all things under the auspices of the Comptrollers' Office and address top-of-mind issues in the Financial Management community.

TOM RHOADS: Good Morning, my name is Tom Rhoads. I'm a Partner with Guidehouse, where I work with clients across the DoD and other government agencies to transform and optimize their financial management functions. I will be your host for today's podcast.

For those of you who may be new to this podcast series, let me take just a moment to provide some background on the American Society of Military Comptrollers. The American Society of Military Comptrollers, or ASMC, is the non-profit educational and professional organization for individuals – military, civilian, corporate, or retired -- involved or interested in the field of defense financial management. ASMC promotes the education and training of its members and supports the development and advancement of the profession of defense financial management. The Society provides membership; education and professional development; and certification programs to keep members and the overall financial management community abreast of current issues and encourages the exchange of information, techniques, and approaches.

And with that, I'd like to introduce today's guest, Mr. Mark Hakun. Mr. Hakun is Principal Director for Cybersecurity for the Department of Defense, Office of the Chief Information Officer. Mr. Hakun is responsible for the definition and execution of the Department's cybersecurity program. He oversees the coordination of cybersecurity standards, policies and procedures with other federal agencies, coalition partners and industry. Most recently, Mr. Hakun served as the Deputy Chief Information Officer for the National Security Agency.

Mr. Hakun is certified in Program Management Level Ill through the Defense Acquisition University. He is also a Certified Information Systems Security Professional (CISSP). Mr. Hakun is a recipient of the Navy Commendation Medal and Navy Meritorious Civilian Service Award. Mr. Hakun graduated from the United States Naval Academy with a Bachelor of Science in Aerospace Engineering. He earned his Master's degree in Aerospace Engineering at the Naval Postgraduate School.

Thanks so much for joining us today, Mark.

MARK HAKUN: Thank you for having me.

TOM: Would you mind sharing with us a little bit about your background, and what brought you to your current role as the Principal Director for Cybersecurity at the DoD CIO?

MARK: I've been at the Pentagon almost two years now, since the pandemic started. Prior to this position, I was serving as the NSA, National Security Agency, deputy chief information officer. I'm a National Security Agency employee on detail to the Pentagon. Been at NSA for 15 years.

All the time prior to the CIO position, I was on the information insurance directory side. A lot of that was working acquisition programs, like public key infrastructure, key management infrastructure.

I would come down to the Pentagon frequently to work on financial drills securing money by a budget process. So, when the position opened at the Pentagon, seemed like a natural fit to my career working with the Pentagon, working with military services.

Prior to my NSA career, I was a naval officer, and then worked acquisitions out in San Diego for what was then the Space and Naval Warfare Systems Command working their computer network defense programs and cross-domain solutions. So again, a natural fit to what I'm now doing at the Pentagon.

TOM: Well, Mark, thank you for your service. It sounds like cyber security and IT infrastructure is definitely a passion of yours.

With the advancements in technologies that are creating additional cyber risks through the use of cloud, multi-cloud and hybrid infrastructures, this coupled with distributed workforces make cyber-attacks more difficult to defend.

In our current environment, what are some of your organization's top cybersecurity initiatives for 2022?

MARK:

Our top initiative for 2022 has been rolling out Zero Trust. Zero Trust now reflects a current state of play with inside the Department of Defense. Given that data is no longer resident just on our networks, or our devices; they're residing in the cloud. They're residing on external devices.

So, implementing Zero Trust is our primary focus in 2022. And it does represent a real paradigm shift for the department.

Expect in the near-term future to see things like micro-segmentation; greater emphasis on analytics that enable our defenders to understand greater volumes of data; and automation to enable faster responses.

The DoD CIO has stood up a Portfolio Management Office. This office will rationalize all the networks across the department, prioritize them, and or implement us on our path to- to engage and move out on Zero Trust in the upcoming years.

In our view, from the DoD CIO, it's not really about that the Portfolio of Management Office has to stand up. It's about coordinating the network of cybersecurity practitioners across all of DoD, and implementing those pillars as part of our Zero Trust reference architecture. So, a large undertaking inside the department.

Hand-in-hand with that is executing on the President's Cybersecurity Executive Order that was signed last May. We are looking internally across the department to better understand our existing cybersecurity capabilities such as sensors, platforms, and identify opportunities for improved collaboration and communication.

DoD continues to build partnerships with the IT and cybersecurity industry leaders to accelerate the adoption of Zero Trust principles, as well as support workforce initiatives to include advanced training of our cybersecurity workforce.

We have partnerships with the DIB that will affect the raising of standards for cybersecurity overall. Much of the technology we use today on a day-to-day basis is not unique to DoD. So, improvements made will enhance the security of all our systems.

TOM: Thank you, Mark. And what are some of the cybersecurity challenges your organization will face in this upcoming year?

MARK: Across DoD we are noticing that the threat is more sophisticated. DoD is focused on threats from advanced adversaries who bring much more sophisticated tools to both competition and crisis. More importantly, these adversaries have shown a willingness to use these capabilities in competition.

This is complicated by the fact that criminal enterprises now have the capability to affect our national interests in ways that were only theoretical five years ago, as the recent ransomware attacks have shown. Securing cloud environments across the department is also a priority and challenge for our office.

DoD will continue to use the blended enterprise and purpose-built clouds. We have more than a dozen of these purpose-built clouds in use today, and have learned a lot as we're rolling these out.

Industry is a partner in this, and we are leveraging their experience to improve how we configure these cloud capabilities. The information we gather, and the way we integrate disparate tools, platforms, and people.

In addition, the Defense Industrial Base is a partner with us as well. We partner through the DIB and gain their understanding by our partnership with CISA, the Cybersecurity Information Security Agency. Our focus is on the DIB partners. But for those not in the DIB programs, CISA is the key resource.

I'd like to highlight a couple organizations with inside DoD that work with us on the DIB on a day-to-day basis.

First there's the Defense Cyber Crime Center, better known as DC3. As the operational focal point for the Defense Industrial Base Cybersecurity Program, DC3 works with over 900 partners that range from small to large DIB-related firms.

The National Security Agency, my parent organization, has a Cyber Collaboration Center that connects with the DIB and the cybersecurity providers to prevent and eradicate foreign cyber threats.

They established collaborative relationships with these private-industry partners to achieve the collective outcomes of detecting and defeating cyber adversaries targeting national security systems, DoD, and the DIB networks.

Additionally, international partners such as NATO, our Five Eyes partners, Korea, Singapore, and others, are critical to the way that the department operates in competition with a crisis.

We have a team meeting almost every week on some topic such as cyber security, engineering, interoperability, personnel, spectrum issues, working with these foreign partners.

Additionally, as much as we need to increase and share spectrum domestically, we also need to work with our allies to figure out how we can do that in their complex environments as well.

TOM: Mark, it sounds like your collaboration with CYBERCOM and CISA is really helping with the Zero Trust principles of both mindset or culture and methodology and strengthening that across the DoD.

Changing gears just a little bit: I know your organization is working closely with the DoD Comptroller to address the cybersecurity deficiencies found during the last financial statement audit.

What are some of the key initiatives that are being put in place to address those challenges?

MARK: There's a memo signed in July of 2019, known as the 12-Star Memorandum called Addressing Access Control Notifications of Findings and Recommendations from the Department of Defense financial audit.

This memo, in summer of '19 was signed jointly by the Chief Information Officer of the DoD, the former acting Chief Management Officer of the Department of Defense, and the Deputy Undersecretary of Defense Comptroller detailed several items requiring mitigation. Some of these items include the use of shared administrator or user access accounts; unnecessary assignment of privileged access; user-assigned conflicting roles and duties and responsibilities; developer access to production programs; and access to production-ready code files.

Our team continues to track the compliance stats with this memorandum. Other items that were relative to this memorandum include a development promulgation of a new Department of Defense Identity, Credential, and Access Management, better known as ICAM; overarching agency-wide policy.

This overarching policy will mitigate a specific notification of finding or recommendations associated with the department's material weakness on access controls.

This policy is entering into the formal staffing process. We expect that process to complete in about a year. This time next year in 2023 we expect that signed out.

While that policy is making it through the process, we are piloting operationalizing the department's ICAM strategy, suite of services, to address the notification of finding and recommendations associated with access control and segregation of duties.

The Defense Information Systems Agency, or DISA, has been compiling the department's ICAM solution, initially focusing on those ICAM services to address the access control issues, to be followed closely by those services, which will address the segregation of duty issues.

Several components including the services of some defense agencies are pursuing component-level ICAM solutions, which will federate to the department's enterprise ICAM solution for addressing access control and segregation of duty to notification of finding and recommendations.

ICAM, coupled with the component-level policies, processes, and procedures, will help holistically address the findings, which in turn will help the department overcome that access control material weakness.

TOM: Do you feel that these initiatives that you're putting in place to bring in line the cybersecurity deficiencies in the audit findings; will these improve collaboration between the cyber security assessors and the FMIT auditors to gain efficiencies for the DoD?

MARK: As you know, the Chief Information Officer team has been supporting the financial audit recommendations. It undertook a research study to determine the deltas between issues discovered during the Risk Management Framework, or RMF system assessments, and the RFD systems. A number of key findings engaged.

But before I address those findings specifically, I would like to express my deep appreciation to the systems owning components who participated in this study. These components are very generous with their time from both their chief information officers and financial management organizations, which made the study a success.

These components included the United States Air Force, the United States Army, United States Marine Corps, United States Navy, Military Retirement Fund Program, United States Army Corps of Engineers, the Defense Finance and Accounting Service, Defense Logistics Agency, Defense Health Agency, Defense Health Program, and the Defense Information Systems Agency.

This study approach included three phases. Phase one was that for each system within the study, compared with independent public accountants' information technology-controlled consistencies from the audit, with RMF documentation from our eMASS regarding similar controls from the NIST framework standards 853, assessing and securing privacy controls in federal information systems and organizations.

Phase two was met with systems authorization officials and system control assessors to gather additional details to understand reasons for the divergences. And phase three identified root causes and documented lessons learned.

Study finds included that, 1., RMF is focused on cyber security and privacy control, and doesn't look at test findings through a financial lens.

RMF testing is focused on test of design and a limited test of operational effectiveness.

RMF information technology controls sample testing is performed on a limited basis, with only a few samples selected and without guidance for those how to perform the testing.

Financial management overlay into department's RMF knowledge service is not implemented as intended.

The mapping between this special pow-853 controls, and Federal Information System Controls Audit Manual, or FISCAM, does not exist.

A limited number of RMF security control assessors and validators assess hundreds of controls in a limited period, compared to external auditors auditing a small number of controls in a longer timeframe. A lack of resources conducts thorough RMF-controlled assessments.

RMF is not designed to address Complementary User Agency, or CUECs. Some component chief information officers and authorized officials are not aware of the information technology audit findings.

And a limited or no coordination communication between the RMF, OMB, the Circular 123, and financial management improvement audit rating seen from information technology, of those audit controls. Remediation of these findings is now underway.

TOM: Well, hopefully it sounds like the RMF overlay will help bring the cybersecurity assessors and the auditors into line to help eliminate future findings going forward. Mark, you touched on this a little bit earlier. Can you tell us a little bit about President Biden's new Executive Order on improving the nation's cybersecurity? And any impact it's had on your strategies or plans?

MARK: The Executive Order 14028 is primarily focused on improving the cyber security of the federal civilian executive branch. Consequently, most of the EO's guidance has confirmed what the department has already implemented, such as multi-factor authentication, or as instituting a Zero Trust cyber security architecture.

We assess that the biggest impact for us is that the EO specifies certain tasks to accomplish within a specified time period, to ensure DoD's national security systems meet or exceed those standards of the federal information systems.

Not surprisingly, the EOs and NSS requirements echo those found in the 19 January of 2022 National Security Memorandum number 8 to improve the cybersecurity of the national security systems of the DoD and the IC.

TOM: Thank you, Mark. Cyber adversaries are getting more sophisticated, security attacks and specifically ransomware attacks have increased dramatically over the pandemic. Has this been an issue for DoD, or any of its industry partners?

MARK: As you've seen in the news over the last few years, there've been a number of major cybersecurity incidents. We have spent a great deal of time identifying and remediating events, such as SolarWinds, Pulse Connect Secure, Log4j. The DoD has been able to manage these responses to these incidents with minimal impact to our network's admissions.

As for ransomware, the DoD has a robust defense and defense in-depth strategy, and the effects of ransomware and networks admission has been minimal. The DoD has not detected any increase in impact of ransomware during the pandemic.

We have and continue information sharing with the Defense Industrial Base sector. We share industry standards on ransomware, mitigation strategies, and through findings with our industrial partners through the DIB's CS program.

TOM: Thank you, Mark. And for our last question, we'd like to wrap up with this: what you know now, and at this point in your career, what advice would you offer to new careerists who are just starting out?

MARK: So, as I reflect on my career, my background was not in cybersecurity. I was a naval officer. I wanted to fly in the mid-'80s, my degrees are in aerospace engineering. I did not picture myself working in the cyber field.

I was part of the last Naval Academy class that did not have to buy their own personal computer. My last active-duty shift was on a shift without a LAN. So, the information on cybersecurity was not on my radar.

So, what I would offer to people starting a new career, is be open to where your career takes you. And not try to force fit it into one specific mission area or area where you think you may be interested in. But let the path take you to someplace to explore where you may not have thought you were going.

But use all the training you've gotten in classes. The experience you've met, the networking you meet through the people. And let the career flow path guide you when something you may not be able to envision, will turn out more interesting than you could have ever imagined.

TOM: That's great advice. Thank you so much, Mark. And again, we really want to thank you for your service and for your time. I know that you have a very full agenda with all that you're trying to- to work within the Department of Defense.

TOM: Appreciate the passion and the energy that you bring to it, and know you're surrounded by a phenomenal team that brings the same passion and energy. And we're grateful for all that you're doing for the department to protect us, with respect to cyber risk. So, thank you so much, Mark.

MARK: Again, thank you for having me. Look forward to further engagements.

TOM: Thank you.