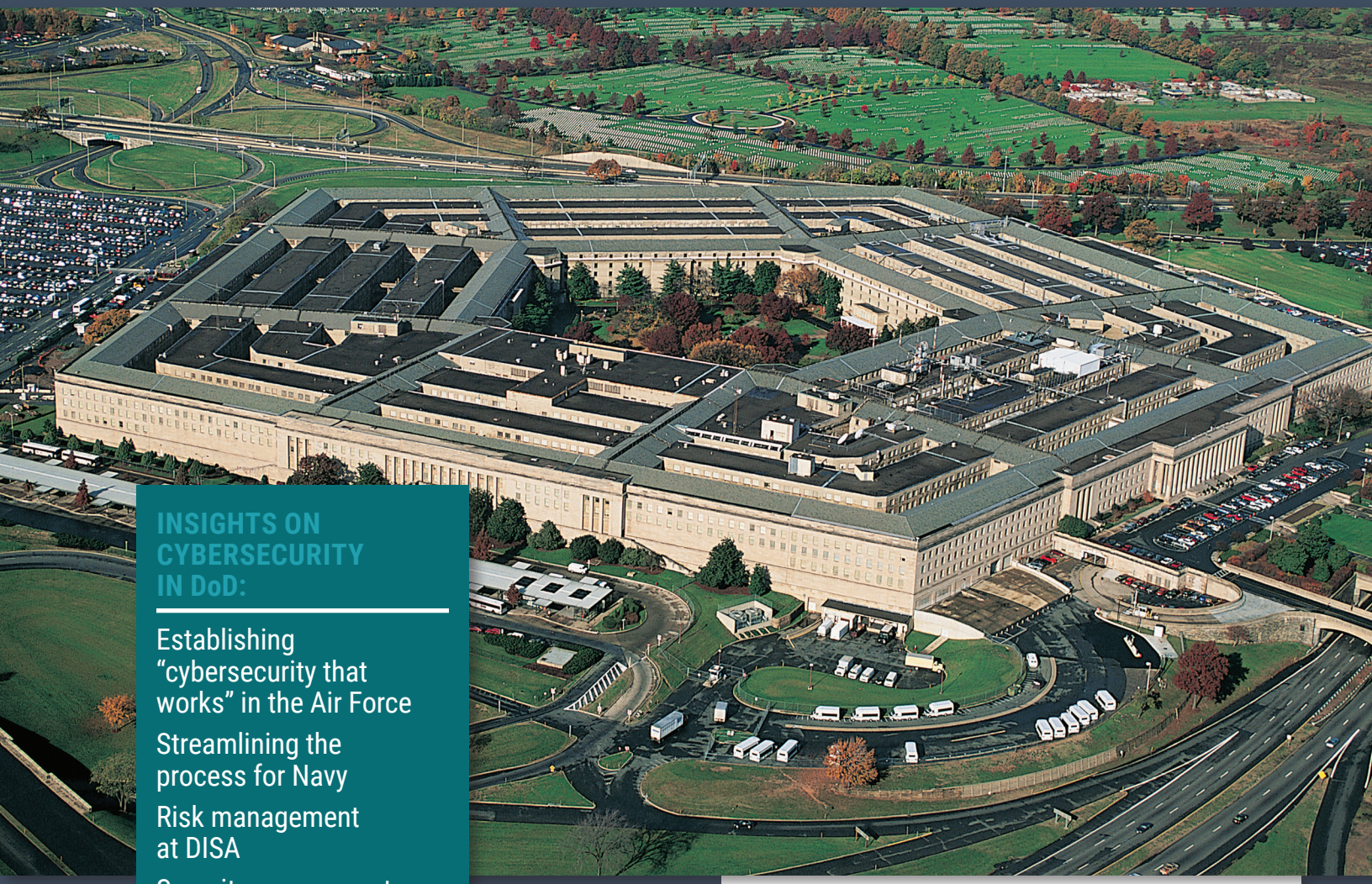
FEDERAL NEWS NETWORK

STRATEGIC GUIDANCE SURVEY:

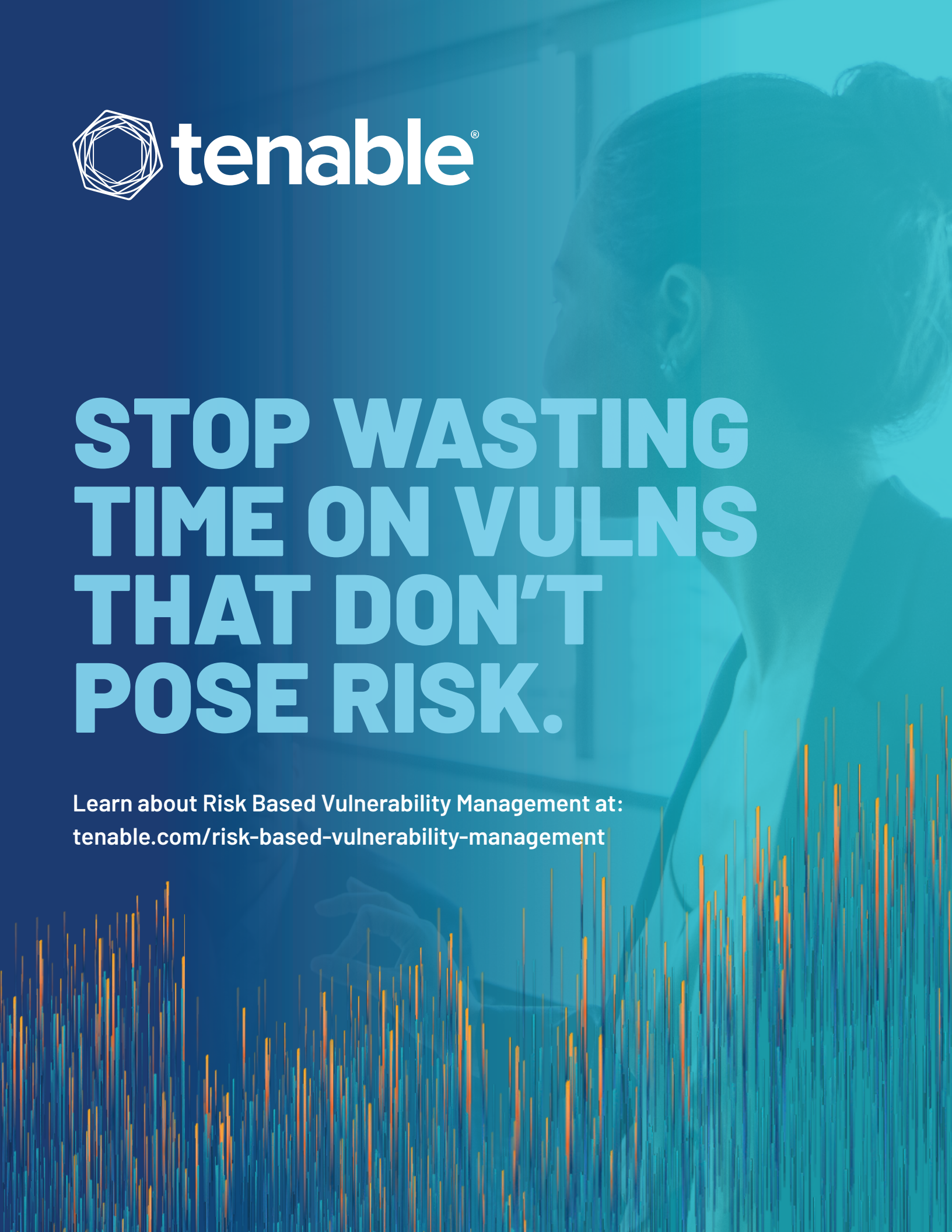
Cyber Technologies in DoD: Protecting Core Infrastructure



INSIGHTS ON CYBERSECURITY IN DoD:

- Establishing "cybersecurity that works" in the Air Force
- Streamlining the process for Navy
- Risk management at DISA
- Security assessment processes assisting the Army
- NIST's plans for updating cyber guidelines

Brought to you by tenable


tenable®
STOP WASTING TIME ON VULNS THAT DON'T POSE RISK.
Learn about Risk Based Vulnerability Management at:
tenable.com/risk-based-vulnerability-management

Risk isn't just a talking point for the Defense Department. In nearly every mission the military services and the Defense agencies undertake, leaders must consider the level of risk servicemen and women and civilian workers face, and how best to mitigate those threats.

When it comes to cybersecurity, the risk calculation and mitigation is an ever-changing battlefield forcing DoD not only to be agile and flexible in how they protect systems and networks, but always looking for new and better approaches.

In this publication, we look at how the Air Force, the Department of the Navy and the Defense Information Systems Agency are doing just that.

The risk management framework (RMF) lets these and other Defense organizations make "operationally-informed risk decisions," as one senior leader told Federal News Network.

We surveyed senior DoD cyber leaders to find out how they are balancing risk and mission, and how those decisions are reshaping their priorities and strategies to deliver services to servicemembers.

SURVEY PARTICIPANTS

Bill Marion,
Air Force Deputy Chief Information Officer

Chris Cleary,
Department of the Navy Chief Information Security Officer

Roger Greenwell,
Risk Management Executive and Chief Information Officer, Defense Information Systems Agency

This e-book also features insights from the Army's effort to fix the initial challenges in moving to the risk management framework. Additionally, the National Institute of Standards and Technology is taking its seminal cyber publication, 800-53, and shifting toward a less static, more risk-based approach based on factors like supply chain, internet of things devices and industrial control systems.

This collection of survey results and articles begin to tell the tale of a changing approach to cybersecurity that has been both a long-time in coming and a sign of the times.

Jason Miller
Executive Editor
Federal News Network

Describe any recent steps your organization has taken to streamline or reform your use of the risk management framework, or, more generally, to reshape your priorities in ways that will let you be more agile in responding to the most serious risks.

AIR FORCE

We have established "cybersecurity that works" as a strategic goal under our fiscal 2019 and 2020 organizational strategy to create a risk-informed approach that enables the commanders to fight and win in a cyber contested environment. Our focus is to empower our senior cybersecurity officials to fuse operational requirements, system forensics and threats to inform risk assessment and tolerance over the system life cycle. The emphasis is on agility and flexibility, as we collaborate with and equip the warfighters with secure capabilities to navigate an increasingly risky cyber landscape.

Reform: While RMF is valuable, its implementation can be a bureaucracy that constrains system fielding in an environment where cyber threats evolve rapidly. Therefore, we have been fully engaged on a variety of efforts that leverage RMF while providing effective and risk-informed cybersecurity.

Specific steps include:

- Introduced the fast-track authority to operate (ATO) process that enables rapid and agile system fielding by leveraging adversarial risk assessment (e.g. penetration testing) and continuous monitoring strategy.
- Established the organizational risk tolerance baseline (ORTB) with the emphasis on critical cyber hygiene risk areas and structured approach to improve the visibility into the cybersecurity posture of the Air and Space Forces.
- Provided policy guidance, which reinforces the paradigm shift on agility while complying with Defense Department instructions and appropriate regulatory requirements. Emphasis remains operations-focused flexibility at scale.
- Created cybersecurity governance structure to ensure collaboration and synergy among the warfighters and cybersecurity professionals.

—Bill Marion, Air Force deputy chief information officer

DEPARTMENT OF THE NAVY

The department is working to modernize and innovate the way we do business and our networks. We recognize our security authorization process must be agile in order for us to roll out these changes while protecting our data. At the DoN level, we are updating our cybersecurity guidance to ensure better alignment with DoD RMF guidance. We are supporting the Navy's RMF reform initiative, which focuses on streamlining the existing RMF implementation process and on defining how we can do a better job assessing and managing risk in the future.

Their RMF streamlining lines of effort (LOEs) focus on:

- LOE 1 - Policy and process
- LOE 2 – Data and automation
- LOE 3 – Workforce development
- LOE 4 – Risk assessment methodology

These LOEs have spawned improvement initiatives across the spectrum of RMF steps and tasks. An associated effort that may bear huge dividends is an RMF automation strategic plan recently released (draft) by Naval Sea Systems Command (NAVSEA). The plan found the worst bottlenecks in the RMF process were caused by the large amount of manual effort required by tasks in two of the steps, and proposed tools that would automate much of the labor saving a significant amount of time and producing more reliable results.

RMF Next, which is still in the concept phase, is intended to improve Navy's ability to assess and manage risk continuously.

—Chris Cleary, Department of the Navy chief information security officer

DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

One of the key areas that the Defense Information Systems Agency is focusing on is our processes around commercial cloud capabilities and the effects this can have for use of the risk management framework as applications move to the cloud.

DISA has the responsibility to support both the Federal Risk and Authorization Management Program (FedRAMP) joint authorization board, as well as the Department of Defense's assessment of offerings. As we look at the information we obtain as part of the process, we're evaluating how to make this information available to mission partners.

We also looking at how to improve the ability for mission partners to see and leverage the information within the enterprise assessment and authorization tools for their risk management decisions. We also are reviewing how we utilize this information as part of the provisioning process, along with how this improved visibility can support the ongoing cyber defense of workloads operating in the cloud.

—Roger Greenwell, risk management executive and chief information officer, Defense Information Systems Agency

Please describe any recent policy (or operational) successes that reflect your ability or demonstrate your plans to accelerate/streamline the assessment & authorization process.

AIR FORCE

The fiscal 2020 strategic goals convey a clear picture of leadership's priorities and focus areas, as we fundamentally enable the digital Air Force to conduct air, space and cyberspace operations. We have also deliberately engaged on a governance structure that improved synchronization at the senior levels to inform better decision-making on cyber and operational risk. Recent policy and operational successes include:

- Changed the flow of risk information – When a senior cybersecurity professional determines a system risk beyond moderate, the chief information officer, senior acquisition officer and owning major command (MAJCOM) commander are informed. This allows for senior stakeholders across the acquisition and operations community to discuss the risks and tolerance, both to the enterprise and to the mission to balance the risk/reward discussion.
- Established a secure baseline of hygiene metrics that establish the Air and Space Forces risk tolerance and streamline the risk management process for a more rapid and effective decision-making.
- The acquisition community has baked cybersecurity into the software development process, expediting and streamlining the fielding process.
- Implemented the fast track ATO process as a primary means within the RMF to make an authorization decision based on performance within an operational environment by leveraging adversarial penetration testing to replicate real-world threats.
- Documented use cases for fast track ATO where senior cybersecurity officials issue an authorization to field and operate systems in two months versus 12-to-15 months using traditional RMF.
- Exploring viability of using fast track ATO for F-35, drones and other non-traditional IT systems. We are increasingly optimistic as the process leverages RMF, but provides more operational rigor through penetration testing instead of a risk assessment based on a paperwork drill.

—Bill Marion, Air Force deputy chief information officer

DEPARTMENT OF THE NAVY

The Navy is working:

- Operation Triton Bastion – transition to RMF by Dec. 31, 2020.
- Process improvement to reduce the number of systems in high risk escalation (HRE Stand Down).
- Updated interim authority to connect (IATT) process that reduces processing time from six months to 45 days.
- Critical assessment of DoD Information Assurance Certification and Accreditation Process (DIACAP) to RMF conversion packages for the fleet identified sufficient rigor was in place to authorize 3-year versus 1-year ATOs.
- As part of the RMF streamlining initiative, NAVSEA developed the RMF automation strategic plan that lays out the goals and current efforts for LOE 2.
- Office of the Chief of Naval Operations (OPNAV) amplifying guidance for required actions and intent with regards to handling expiring authorizations to operate (ATOs) during COVID-19
- Updating Navy RMF process guide to implement changes that reduce processing time by 2-to-4 weeks

—Chris Cleary, Department of the Navy chief information security officer

DISA

DISA, as well as the entire DoD, is undergoing numerous challenges related to coronavirus.

As an example, DISA had to rapidly provision communications capabilities to support the Navy hospital ships. We executed emergency leases of commercial circuits to support communications for the USNS Mercy and USNS Comfort, which required rapid authorization activities to support critical communications capabilities.

In order to enhance the DoD's ability to telework, DISA also worked closely with U.S. Cyber Command and DoD CIO to establish the commercial virtual remote environment to support web conferencing, chat and document collaboration. This effort required a detailed analysis of the risks that drove the design and integration of security capabilities that led to an acceptable risk posture and authorization for use across the DoD.

While these efforts are certainly outside of the normal processes, the efforts highlight opportunities where we need to analyze our processes and determine where we can take risks in deploying new capabilities.

—Roger Greenwell, risk management executive and chief information officer, Defense Information Systems Agency

Assuming the premise that not all risks are equal, what are the most important factors you consider (i.e., asset criticality, severity of vulnerabilities), or questions you ask about a system, network or application when thinking about how to manage risks?

AIR FORCE

We focus on identifying risks and impacts to the enterprise and mission. From the enterprise perspective, we are attentive to the long-term impacts to the larger Air Force – understanding that infected data or information can have a cascading impact across the entire enterprise. From the mission perspective, risk tolerance is balanced with missions. This required a paradigm shift from compliance to a pre-determined set of controls, to now making operationally-informed risk decisions. Compliance provides a false sense of security, as risk is temporal and influenced by changing set of considerations.

We use threat and intelligence information to prioritize the risk. When we identify the vulnerability, its impact (low, moderate, high) and the threat vectors (e.g. internal – disgruntled employee; external – from script-kiddies to state-sponsored entities; to natural – tornados, storms), we can place appropriate mitigations to counter exploitation of those vulnerabilities. We focus on the risks that matter first, such as the critical cyber hygiene areas, which are documented risk areas that increase the security of our systems and missions.

The questions posed to a system, network, or application in consideration of managing risks include:

- What is the value of the information and asset that is being protected?
- What is the impact to the mission in the event that the information or asset is compromised?
- Who or what are the potential threat vectors that could exploit a potential vulnerability?
- What is the likelihood that potential vulnerabilities will be exploited?
- What is the level of risk my organization is willing to accept?

—Bill Marion, Air Force deputy chief information officer

DEPARTMENT OF THE NAVY

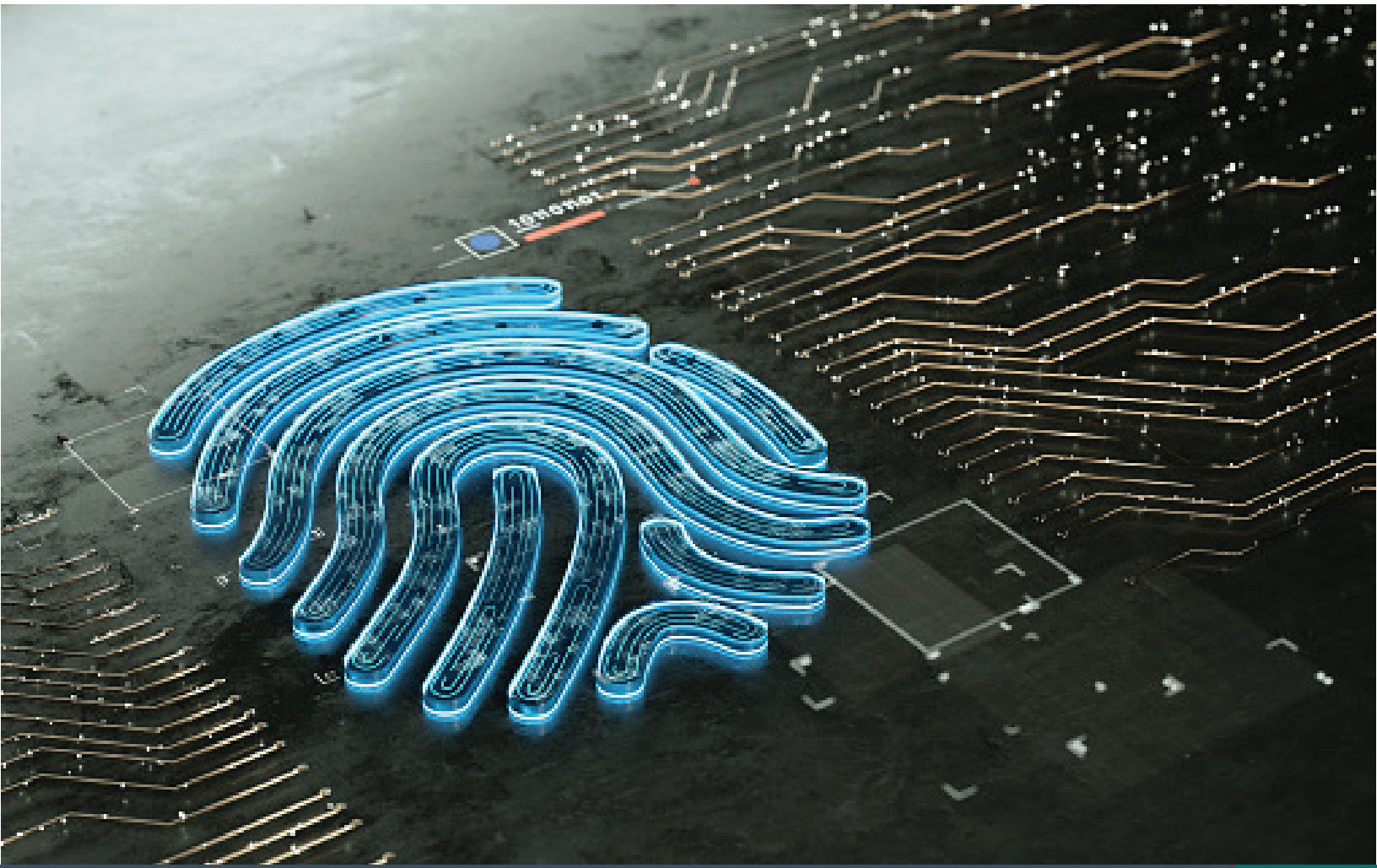
All risks are not created equal and we're really focused on two categories – risk to the Navy's portion of the DoD information network, and risk to mission.

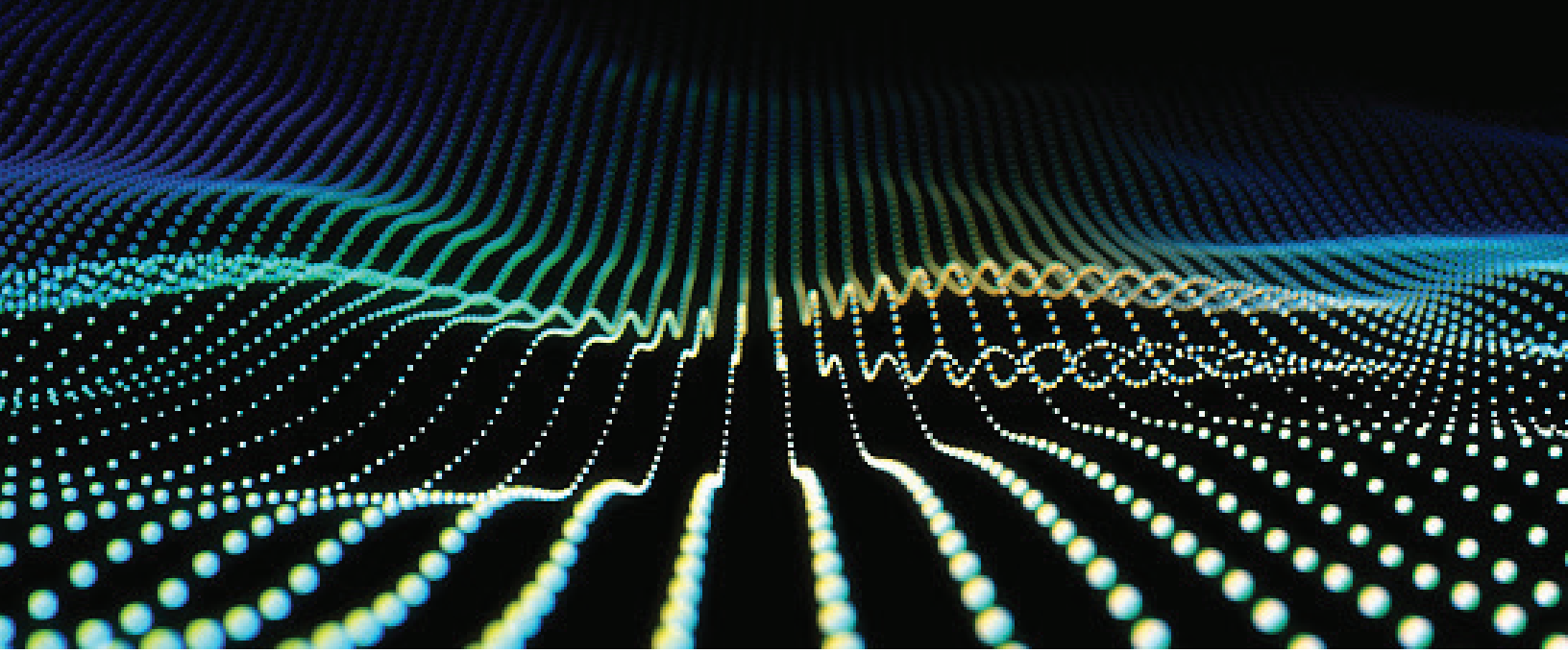
For both categories of risk, it's important to consider three primary factors: vulnerability, capability to exploit the vulnerability and intent to exploit the vulnerability. Assessing known vulnerabilities and determining how or whether our defense in depth measures help protect those vulnerabilities from exploitation is fairly straight forward.

If there is an open threat vector, determining whether the capability and intent to exploit the vulnerability exists is much more challenging. Given the resource constraint environment that we face, it is essential that threat reports and intelligence are leveraged to the maximum extent possible when having a discussion about risk.

Protecting and securing those capabilities and systems that are of particular interest to the adversary would naturally be a priority. We are actively using multiple information sources to inform that part of the risk assessment and recognize that this is an area that requires continued attention.

—Chris Cleary, Department of the Navy chief information security officer





DISA

We consider numerous factors as part of a risk decision. It's not a simple process or answer.

First, we need to understand the impetus and the process driving the decision. For example, is this system being moved from test to production? To what degree has an existing production system been upgraded? Are we updating a software package or are we adding capabilities? Is it an ongoing risk authorization decision? Each of these will bring their own conditions that affect the risks. We also need to understand the operational impact of the decision. If we're adding capability, how critical is this to the mission? If we don't accept the risk, what is the potential impact?

For each of the scenarios, we use several factors in weighing the risks:

- Is the system internet-facing or restricted to the internal network?
- What is the current patching status? Are there critical or high vulnerabilities? How old are the vulnerabilities?
- How is the system accessed? Is continuous authentication in use?
- Is there consistency in how the system is managed? How often is the system upgraded?
- How complex is the change? Can it be readily backed out if problems are identified?
- What level of testing has been done in preparation for the change?
- To what extent are supporting protection capabilities in place? Is host-based protection in place? Are host-level intrusion detection system and intrusion prevention system capabilities affected by the change? Is there a web application firewall in place?
- What ports and protocols are used? Is a demilitarized zone construct in place?
- What code practices are in place? Do software flaws/vulnerabilities exist?

To summarize, risk management, as opposed to risk avoidance, is complex. We have to consider all of these factors and the impacts on operations as we make risk decisions and establish conditions resulting from the analysis of risks.

—Roger Greenwell, risk management executive and chief information officer, Defense Information Systems Agency

How mature do you believe your organization is in its ability to realistically and holistically assess cyber risks across the entire spectrum of "traditional" IT systems AND other connected systems (IoT devices, ICS, weapons platforms, etc). Considering that entire attack surface, what strategies do you use to decide how to prioritize your defensive cyber investments?

AIR FORCE

We have been fully engaged on strengthening our cybersecurity posture across the entire spectrum. We are in the process of collaborating with our mission partners to address the cybersecurity strategy and initiatives for our connected systems, and we have integrated their senior cybersecurity officials into our cybersecurity governance process. The studies chartered by the Defense Authorization Act Sections 1647 and 1650 have provided extremely valuable insights on the risks to our weapon systems and ICS.

As the landscape gets more interconnected and complex, the drive for innovation can create potential seams, which introduce additional risk vectors. We push through the challenges using strategy development such as cybersecurity strategy, cloud strategy, cybersecurity service provider strategy; endpoint management; enterprise IT-as-a-service; and collaboration and synchronization with numerous mission partners such as intelligence, acquisition, operations, chief data officer, installation support and risk executive function.

—Bill Marion, Air Force deputy chief information officer

DEPARTMENT OF THE NAVY

The Navy and Marine Corps teams are very mature in their ability to assess cyber risks across the entire spectrum, including weapon systems/platform IT (PIT), enterprise systems, mobility (phones and tablets), ICS, etc. We've been doing this a long time.

Having said that, there is always room for improvement. RMF is not perfect, but it's an improvement over DIACAP, and efforts to improve both RMF and our execution of RMF process are continuous. We're finding ways to streamline the RMF process, identifying the bottlenecks in the process and considering solutions and tools which will increase efficiency, while simultaneously developing a new approach that will increase the effectiveness and efficiency of our risk management.

One of my primary responsibilities as the DoN CISO in the defend track is to integrate the myriad reports and assessments in order to be able to explain to the CIO and Secretary of the Navy the overall cyber risk posture for the entire DoN. We're getting better at collating the data necessary to inform their understanding of our risk posture, but this is definitely an area that needs improvement.

Our investment strategy to reduce the overall attack surface has centered on the identify-protect-detect-react-restore framework. This has included ashore, afloat, and air networks. We prioritized them based on the priorities laid out in the National Defense Strategy and based on cost effectiveness. The aim for these investments is to provide mission assurance in a cyber-contested environment across critical warfare areas.

—Chris Cleary, Department of the Navy chief information security officer

DISA

As we look across the spectrum of what DISA provides to the warfighter, we have to ensure that the warfighter has the necessary capabilities to operate, both from an availability as well as a security perspective.

Within our data centers and network control centers, we depend on control systems to ensure the integrity and security of the facility itself, whether that's controlling access, fire suppression, heating, ventilation and air conditioning or power, just to name a few.

DISA provides critical communications capabilities at multiple levels of classification across varying communities of interest and coalitions, across numerous technologies ranging from leased lines to satellite, and everything in between. Systems and networks support missions ranging from public information systems to business systems to command and control at all levels of the government.

As we look to optimize our investments and bring more powerful capabilities to the warfighter, we're continuously reviewing the threats, the advancing capabilities of our adversaries and the evolution of technology to prioritize our investments. Just as important, one of our key focus areas is to ensure DISA's capabilities are "always on" and available to support the mission. Identifying potential single points of failure across the entire spectrum of services and capabilities to ensure mission success is another important driver for our investments.

—Roger Greenwell, risk management executive and chief information officer, Defense Information Systems Agency

How would you assess the capacity and capability of your organization's IT and cyber workforce to manage vulnerabilities in a risk-informed way? What steps are you taking to overcome any challenges in this area?

AIR FORCE

Given the fiscal and resource constraints, our workforce remains committed to mitigating the appropriate risks to assure mission success. We are engaged in various lines of effort to navigate the challenges through innovative and agile processes, Digital University for our airmen and leveraging existing capabilities, such as cyber technical orders, cloud, and mission defense teams to strengthen our cybersecurity posture.

The Under Secretary of the Air Force signed a memo introducing fast track ATO and encouraging the cybersecurity community to shift from a compliance focused model to a risk-based model tied to mission success. We are continuing to institute measures to reinforce the culture shift as we work through the funding challenges.

—Bill Marion, Air Force deputy chief information officer

DEPARTMENT OF THE NAVY

The DoN has a talented and mission focused IT and cyber workforce dedicated to manage vulnerabilities in a risk informed way. That said, it is no secret that cybersecurity personnel are in high demand and that the government is competing with industry to retain talent.

To attract and qualified candidates, the Navy has begun new and expanded existing initiatives to recruit, train and retain the cyber workforce. Recruiting, developing and managing cyber workforce talent in the information age are key themes in every federal and Department of Defense (DoD) cybersecurity policy.

DoN CIO Aaron Weis, myself and the team are committed to building the future leaders today. Our future leaders need to come from within. The future DoN CIO is a junior sailor, Marine and civilian today!

—Chris Cleary, Department of the Navy chief information security officer

DISA

DISA has some of the most conscientious and knowledgeable cyber professionals I've worked with throughout my career.

Our chief engineer's panel, which is made up of all the technical directors from across the organization, works together to review and advise our engineers in building and operationalizing secure and robust solutions to meet the DoD's needs. Our cyber assessment teams work closely with program managers, security managers and engineers to assess risks and guide priorities for reducing the overall risks.

From the teams that develop policy and technical guidance to the program managers and engineers that build and manage DISA's services to the operations team who provide the frontline cyber defenses, the workforce operates as a cohesive team to share knowledge and develop approaches to identify and manage risk on a continuing basis.

DISA also has an established, robust cyber intern recruiting and development program to meet future workforce demands. This effort is truly an agencywide program that begins with establishing relationships with universities and even high school students. Educating them about the importance of our mission, the opportunities that exist throughout the agency and the sense of accomplishment and pride that comes from supporting our nation's warfighters is the key to successfully recruiting and retaining new talent. DISA's ongoing developmental programs focus on helping interns, as well as our current cyber workforce, understand the mission and provides continual cyber training opportunities, both formal and informal, with the goal to match interest and expertise across the agency.

—Roger Greenwell, risk management executive and chief information officer, Defense Information Systems Agency

Army's Project Sentinel aims to fix RMF authorization bottlenecks

It's been five years since the Defense Department adopted the risk management framework as its new method for accrediting the cybersecurity of IT and weapons systems. And to put it gently, things got off to a bit of a rocky start. In the Army's case, because of the way the service first implemented RMF, it resulted in an 800% increase in workload.

But officials said they've already made dramatic improvements in the process even as they're now setting out on a multi-year, three-phase RMF reform effort called Project Sentinel. The Army says it has shaved hundreds of hours off the authorization and accreditation process and eliminated its backlog of systems awaiting cyber approval.

"I think we're at the point now where we've learned enough, and you see this in the other services as well: the Air Force did their Rapid ATO process, and we did a similar process for our tactical systems," Nancy Kreidler, the director of cybersecurity and information assurance in the Army CIO's office said in an interview with Federal News Network. "There was a really steep learning curve and it did take a while to get a handle on the process before we started tailoring."

By "tailoring," Kreidler means taking the full body of security controls in RMF — there are some 1,900 in all — and prioritizing the ones that are most critical to the Army or to the security of a particular system, considering the environment that system will operate in.

That is a marked departure from how the service first adopted the framework, which was developed by the National Institute of Standards and Technology.

In 2015, when the Army first switched to RMF, it began using its own workforce to conduct security assessments, rather than the third-party assessors who were hired to do the job under the former DoD process, known as DIACAP.

"What happened was there were so many controls and they were not prioritized," Kreidler said. "Every control becomes equal to the control before and the control after it. And because of that, you really aren't prioritizing your risk or what you should focus on. And when you go from maybe a 200- assessment procedure to 1900 assessments, you just try to get through the process."

The NIST process explicitly calls on organizations that use RMF to start by selecting the controls that are relevant, and that's what the Army is largely doing in the first two phases of Project Sentinel.

In the first phase, the Army is looking at ways to let individual systems "inherit" security controls from the infrastructure they operate on, or from policies that are already enforced across the entire organization.

"An example would be do you have acceptable use addressed in a policy? We do. We have a privileged access policy, and so we can answer this control once and then all systems can inherit that answer," Kreidler said. "And so while this may look very small, the fact that you don't have to answer a control for every system in the Army over and over saves a huge amount of time. We are going to continue to look at this control set and see where we can either use inheritance and answer once for the Army, or we can consolidate."

A working group of RMF experts from across the Army hopes to agree on a smaller, consolidated set of security controls that most systems will be assessed against. Kreidler said it's

impossible to know exactly how many there will be, but she hopes to reduce it from 1900 to between 200 and 300.

"It's not about just reducing the controls that we're really looking at, it's identifying the right controls based on what we need. One of the things that I want to ensure is that when we reduce this control set, it is the right controls and we can hold people accountable," Kreidler said.

Beyond consolidation, the Army will focus on prioritizing the controls its assessors look at in phase two of Project Sentinel.

To make decisions about which of the controls are most vital and where it is and isn't willing to take risks, it will use threat data from Army intelligence, the Center for Internet Security and other sources.

"We will continue to identify these threat sources as time goes on, and we're going to map the current threat to the controls and prioritize the controls," Kreidler said. "Once we do that, we're going to identify a threshold depending on what's going on in the state of cybersecurity. And there will be instances where there are vulnerabilities that are found that cannot be mitigated without a higher level review. An example of this would be personally identifiable information that is not encrypted. Are we going to allow that on the network or not?"

In the project's third phase, the Army plans to conduct its own rewrite of the NIST security controls so that they're more understandable to its own assessors and other stakeholders.

"This is important because you can have five people in a room looking at a NIST control and you will have five different interpretations of what it's asking for," she said. "Sometimes it's just putting it in plain language. But there's other specific instances in the Army, for example, on tactical systems, where a NIST control may ask something that doesn't really fit into that architecture that you're looking at. An example might be it's asking for something about the physical environment, but the system is a [portable] radio. Well, you can't really answer that question. So is there a way we can write that in a way that we either understand what the control is really asking for, or write it in a way where the person can address it?"

The Army has already seen significant time savings in its security assessment process during the initial phase of the reform effort.

For example, by letting systems take credit for policy-based controls, it's cut 167 separate procedures from the list of items its assessors must tackle. The service estimates that's saved about 40 hours of work for each system — and the Army has about 1,000 systems that are subject to RMF. And it's managed more reductions among the tactical systems the Army's cross-functional teams are working on, cutting an average of 230 hours of work per system from those projects.

For vendors, the changes are likely to mean that systems that are built with RMF in mind are the ones that are most likely to gain security approval more swiftly.

"This is going to really look at systems and applications and networks where security is built in, because if it's not built in, it's going to show in this process," Kreidler said. "In the past, things were able to be documented in a plan of actions and milestones. If you come with a system or a product that is above our risk threshold, we're going to have a little bit more difficulty getting it on the network."

In major update to key security guide, NIST aims to make security controls more 'dynamic'

It's taken some time, but the military services and other DoD components have broadly come to the realization that using a checklist mentality to authorize and accredit the cybersecurity of their network-connected systems is a recipe for delay, and for suboptimal security too.

But even as Defense authorizing officials adjust their procedures to account for only the security controls that are relevant to the system or network they're trying to accredit, the National Institute of Standards and Technology is trying to make that job easier.

As part of a major revision of Special Publication 800-53 – the key document that underpins the government's risk management framework and numerous other federal cyber policy guides – NIST hopes to implement a "dynamic" catalog of security controls.

When the next update, revision 5, is published later this year, it will include a pivot to online delivery. Instead of sifting through a static, 480-page list of security controls, federal authorizing officials will be able to pick out only the ones that apply to the specific cyber problem set they're looking at.

"The ultimate vision is to be able to have you go to our website and search the entire control catalog, select controls, build security plans, and do a lot of this online where a lot of that volume will be transparent to you. You'll be able to go to only the things that you need," said Dr. Ron Ross, a NIST fellow who has long led the agency's federal information security efforts. "It will also allow us to update the security and privacy controls more frequently. If we see a new threat, or if there's a new cyber attack, we can develop a control quickly, we can get it up online, and we can put it into a beta test."

NIST released the final draft of its forthcoming update to SP 800-53 for public comments in March, and continued to gather input up through May 15. As part of that process, the agency has been trying to get feedback from DoD and other agency stakeholders about how well the security procedures NIST has outlined map on to the real-world systems they're trying to deploy.

"The reviews are just invaluable. They help us determine whether the controls and the content in our pubs are implementable by folks on the front line," Ross said.

The 800-53 rewrite also includes some major new focus areas, many of them responding to the government's experience with cyber attacks in recent years, plus long-term feedback from DoD, the intelligence community and the Department of Homeland Security.

In particular, the latest draft revision includes a new emphasis on supply chain risk management and deeper guidance on how to integrate federal requirements on cybersecurity with those that deal with privacy. And even though NIST plans to make its catalog "dynamic" to deal with emerging cyber threats, the latest revision also points toward the need to build systems that are resilient against cyber attacks over long periods of time.

And in addition to pressing agencies to think about cybersecurity over longer time horizons, Ross said NIST has also tried to build cyber guidelines that apply across the breadth and depth of systems they're connecting to their networks – from traditional desktop computers, to industrial control systems, to Internet of Things (IoT) devices.

"The controls have to be technology and policy neutral, and this has been kind of a confusing point over the years," Ross said. "As we start to develop different types of technologies, for example, cloud computing, or mobile, or IoT devices, many people ask us, 'Where are your controls for those types of technologies?' And the answer is, they're the same controls that we've always used – they're just applied in a different way to the particular technology."

A good example of that, he said, is the government's Federal Risk Authorization and Management Program (FedRAMP) certification program for commercial cloud computing services. That framework uses 800-53 as a baseline, but it's tailored to hone in on the security controls that are relevant to cloud.

"You can also apply these controls to devices that are smaller form factors, like smartphones. But they're always tailored to meet that that specific technological need, and the same thing will happen with IoT," Ross said. "As we start to move to smaller and smaller devices and we're sending computers out to the edge, all of those technologies that are being innovated by industry, these controls will always be there to be implemented in that particular technology – with some tailoring, of course."

tenable

SOLUTION OVERVIEW

RISK-BASED VULNERABILITY MANAGEMENT

Business challenge

Thanks to the rise of digital transformation, everything is now connected. Cloud and containers, operational technology and mobile devices – something new is popping up every day and it all must be included in the scope of your vulnerability management program. But, your growing attack surface makes the vulnerability overload worse. You know the problem: The more broadly, frequently and thoroughly you assess all your assets (which is the right thing to do), the faster you bury yourself and others under a mountain of vulnerabilities and misconfigurations. It's tempting to do less and just meet the compliance requirements. But, less is less, and it puts your organization at risk. Old approaches to vulnerability management are no longer sufficient. You need a way to identify all the vulnerabilities – and then winnow them down to a manageable quantity.

Solution

A proactive, risk-driven approach delivers comprehensive, continuous visibility and informs technical and business decisions. You need a solution that helps you:

Assess all your assets for vulnerabilities and misconfigurations continuously

Measure the vulnerability's risk to your business using threat intelligence and asset criticality

Predict which vulnerabilities present the most risk to your organization, so you know what to focus on first

Deliver risk-based information to business owners

This is risk-based vulnerability management, and it's not optional.

Value

Risk-based VM is the process of reducing vulnerabilities across your attack surface by prioritizing remediation efforts based on risk. With the Tenable Risk-Based Vulnerability Management Solution, you get:

- Full visibility into the converged attack surface: Get the broadest coverage and most thorough assessment of the traditional and modern assets in your attack surface.
- Dynamic and continuous assessment: Assess new and transitory assets as soon as they become active (e.g., integrate assessment into your CI/CD pipeline).
- Prioritization powered by machine learning: Know exactly which vulnerabilities to remediate to reduce risk. Our machine learning models automatically combine vulnerability severity data with threat intelligence and asset criticality to predict each vulnerability's impact on your organization.
- Tailored dashboards: Communicate business system risk, not vulnerability counts, to business stakeholders.

THE CYBER EXPOSURE LIFECYCLE FOR RISK-BASED VULNERABILITY MANAGEMENT

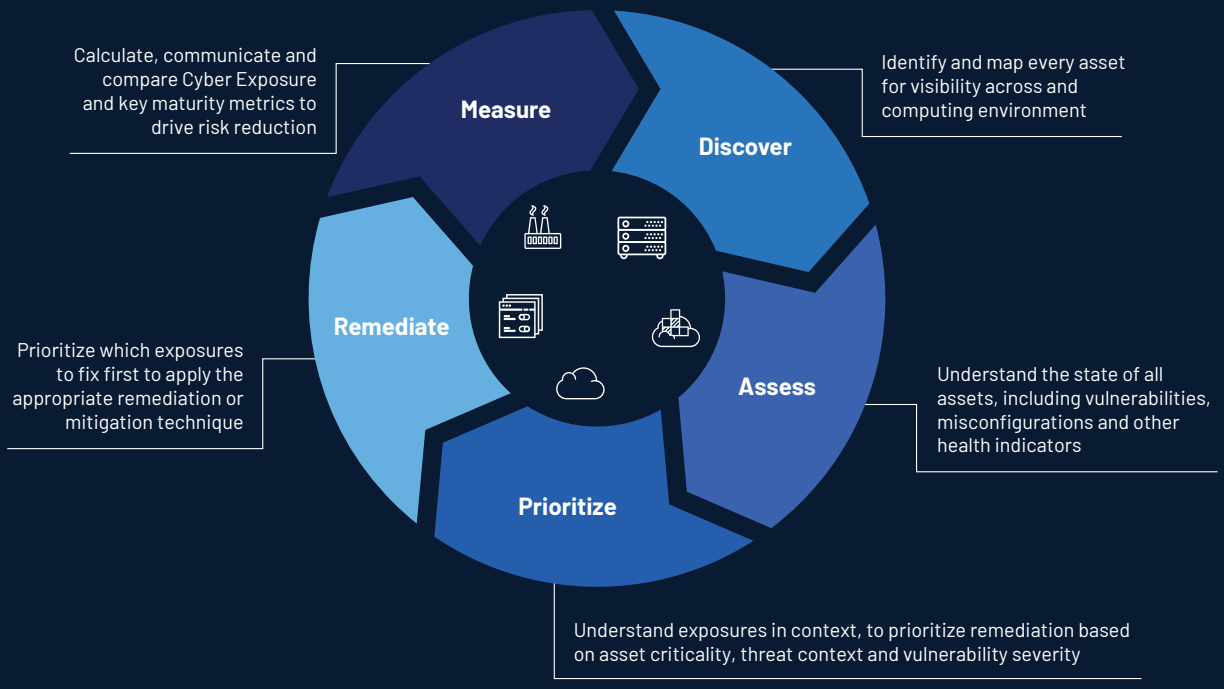


Figure 1. The 5-Step Cyber Exposure Lifecycle for Risk-Based Vulnerability Management

How it works

The Tenable Risk-Based Vulnerability Management Solution is built upon the five-step Cyber Exposure Lifecycle, which helps you continuously improve your security program (see Figure 1). Applying the solution via this lifecycle will help you get complete visibility into your attack surface and prioritize your remediation efforts based on the 3% of vulnerabilities that pose the greatest risk to your organization – reducing your cyber risk over time.

Get started with risk-based vulnerability management today

Upgrade from traditional VM to managing and measuring cyber risk with the Tenable Risk-Based Vulnerability Management Solution. Visit our solution webpage to learn how we can help you evaluate your current VM capabilities, assess gaps in your program and develop a plan to begin adopting risk-based VM best practices today.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

tenable®

02/24/20 V02