

# Securing Data

# for **CYBER RESILIENCY**

## INSIDE:

- Data Security at DOD .... 3
- NIST's Framework  
for Secure Data  
Architectures ..... 6
- Human-Centered  
Design's Role in Cyber ... 7
- FDA Medical Device  
Security ..... 11

SPONSORED BY

**maximus**

# From the editor's desk



Ross Gianfortune, Managing Editor

## Useful Data Needs to be Secure

Agencies collect, store and analyze reams of data each day, which is why keeping it secure grows evermore important amid growing threat environments. Leaders from the Food and Drug Administration (FDA) and the Defense Department (DOD) recently discussed how they are approaching these issues.

DOD's Information Network (DODIN) is one of the largest in the world. The agency created a new system called CORA to continuously assess the cybersecurity posture of its network. Unlike inspection-based systems, continuous systems are more secure, produce better assessments and

better protect data, Defense officials say.

At FDA, securing patient data is critical especially for medical devices. Officials are working with international allies and partners to safeguard patient data and ensure the integrity of connected medical devices.

A key part of securing data in systems is aligning to the National Institute of Standards and Technology's recently updated rules for protecting sensitive information, including guidance for capabilities used in data confidentiality reference design to ensure safe storage. ✨

# Table of Contents



Jordan McDonald,  
Staff Writer



Dana Klosner,  
Staff Writer



Michaela Scott,  
Staff Writer

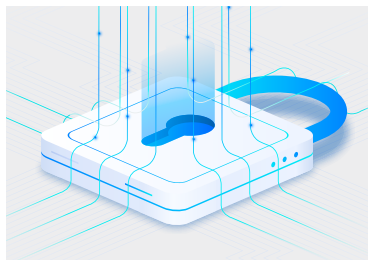


ARTICLE

## DOD Has a New Cyber Resiliency Assessment Program

Defense officials tout the continuous assessment feature and scalability of the new program amid increased cyber threats.

BY JORDAN McDONALD & DANA KLOSNER



INFOGRAPHIC

## Capabilities of Updated NIST Guidelines for Protecting Sensitive Information

The National Institute of Standards and Technology's guidelines for protecting sensitive information includes reference design that identifies and protects assets from unauthorized access and disclosure. The capabilities play a role in protecting data and mitigating confidentiality attacks.



PARTNER INTERVIEW

## How Data Management and Human-Centered Design Improve Data Security

Developing a robust data security strategy starts with good data management techniques and a holistic view of how users interact with data.

**Kynan Carver, Cybersecurity Lead, Maximus**



ARTICLE

## FDA Eyes Global AI Partnerships to Safeguard Patient Data

The Center for Devices and Radiological Health director warns Congress of national security implications if the U.S. restricts AI development in medical settings threats.

BY MICHAELA SCOTT

# DOD Has a New Cyber Resiliency Assessment Program

Defense officials tout the continuous assessment feature and scalability of the new program amid increased cyber threats.

BY JORDAN McDONALD & DANA KLOSNER

Defense Department officials say its new system to continuously assess cybersecurity posture of its network emphasizes more agility and resiliency to keep up with evolving security threats and help meet department goals toward Combined Joint All Domain Command and Control (CJADC2).

Launched in March 2024, the Cyber Operational Readiness Assessment (CORA) program finished a nine-month pilot to replace its legacy system. Officials said the prior system, the Command Cyber Readiness Inspection (CCRI) program, was unscalable because of the sheer size of the Department of Defense Information Network (DODIN)'s global makeup of over 15,000 unclassified and classified networked and cloud environments across combatant commands and services.

“CCRI was a great method that was very rigid. It had a rigid scoring model with rigid checklists,” Charles Wille, deputy director for readiness and security inspections at Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN), told GovCIO Media & Research. “But this cyber domain demands agility. Things change very quickly. The adversary turns on a dime. So, we need to turn on a dime. We need to be able to change that assessment criteria not in months, but in days or weeks.”



### Automation and AI Could Ease CORA Assessments

Wille added that AI could play a role in helping identify potential threats or risks or even help with grading agencies' ability to detect, defend and respond to emerging threats. (ctd.)



# Charles Wille

Deputy Director for Readiness and Security Inspections, JFHQ-DODIN

“There’s two veins to this: You have AI for cybersecurity in one, and cybersecurity for AI. We have this challenge here, but in this vein, we need both. We need to make sure that, as we employ AI technology, that they’re secure. And we need to leverage AI capabilities for cybersecurity,” Wille said.

“We’re looking for ways to automate that and do it at a continuous basis,” added Nicholas DePatto, inspections branch chief at JFHQ-DODIN. “How can we automate what we’re doing? There’s going to be manual parts to everything. But if you can automate 80% to 90% of the [CORA] assessment, you could do it.”

## **Moving Toward Continuous Security**

CORA helps the department move away from a compliance-focused cybersecurity mindset and pushes commanders to holistically and continuously assess how a cyber risk will affect mission.

JFHQ-DODIN leads DOD’s unified force approach to network operations, security and defense on behalf of CYBERCOM. Officials say the component is a key player in executing the department’s CJADC2 strategy as it looks to take on cyber threats abroad before they affect systems and information at home.

Unlike an inspection-based system like CCRI, continuous assessment systems are more secure and produce better data.

“In order to get continuous, holistic assessments of terrain using capabilities, we need to look at our current future emerging technologies along the way,” Wille added. “Let’s say we have the capabilities we have today — are they telling us the truth? We do a CORA at places that matter, and we have this dataset that enable us to look at what we thought to be true about risk against what is true, and it allows us to fine tune those capabilities.”

## **Continuous Assessment Underpins Modern Cybersecurity**

DePatto said in February that “technology changes so frequently, so fast, it’s hard for everyone else to keep up. A vulnerability that we are not even aware

about today, right now, is probably being exploited in the wild. With the flexibility of CORA, we're able to shift and adapt and overcome to start focusing on those unknown or newly discovered vulnerabilities for what is important to JFHQ-DODIN because of intel and threat reporting."

He added CORA could reach a point where continuous assessments are happening in the background without interfering with an employee's normal work day. Eventually, a risk score report could be generated and delivered to commanders and directors to help them understand risk within the agency and where to specifically focus efforts closing gaps in security.

"The end goal is having continuous assessments and continuous monitoring of those critical capabilities within those critical assets, to really give you a day-to-day understanding," said Lt. Gen. Robert Skinner, director of the Defense Information Systems Agency (DISA) and commander of JFHQ-DODIN, earlier this year.

Wille implored those being assessed by CORA to work with their assessors to improve the process.

"We have to come to this mindset that we need to assess, we need to harden, we need to be resilient. The assessor is not your adversary. We need to bring that downward, inspection to assessment. ... We know who the adversary is and that's not the assessor."

Skinner said that while CORA was progressing, it had run into some expected "bumps in the road" around training and assessment expectations.

"The level of cybersecurity posture we're driving to a higher level, and so they just weren't ready for that. But it's a good thing, because now they know, and the posture is already increasing across the enterprise," Skinner told GovCIO Media & Research. "The good thing is that we've learned from the first ones that we've done. We've been able to share that with everyone else and they already know what the expectation is and what the standards are for future assessments." ❁

**“We have to come to this mindset that we need to assess, we need to harden, we need to be resilient. The assessor is not your adversary.”**

**— Charles Wille, Deputy Director for Readiness and Security Inspections, JFHQ-DODIN**

## Capabilities of Updated NIST Guidelines for Protecting Sensitive Information

The National Institute of Standards and Technology's guidelines for protecting sensitive information includes reference design that identifies and protects assets from unauthorized access and disclosure. The capabilities play a role in protecting data and mitigating confidentiality attacks.

**DATA MANAGEMENT** allows discovery and tracking of files throughout the enterprise.

**DATA PROTECTION** involves encryption and protection against disclosure of sensitive files.

**ACCESS CONTROLS** allow organizations to enforce access control policies, ensuring that only authorized users have access to sensitive files.

**BROWSER ISOLATION** protects endpoints in the organization from malicious web-based malware by sandboxing and containing executables downloaded from the internet.

**POLICY ENFORCEMENT** ensures that endpoints in the organization conform to specified security policies, which can include certificate verification, installed programs and machine posture.

**LOGGING** creates a baseline of normal enterprise activity for comparison in the event of a breach.

**NETWORK PROTECTION** ensures that hosts on the network only communicate in allowed ways, preventing attacks that rely on direct communication between hosts and those that use side channels. It also protects against potentially malicious hosts joining or observing traffic on the network.

PARTNER INTERVIEW

# maximus

## How Data Management and Human-Centered Design Improve Data Security

Developing a robust data security strategy starts with good data management techniques and a holistic view of how users interact with data.

 **How do customer experience, user experience and human-centered design principles play a role in measuring data use and availability, and why is this important for data security?**

**Carver** Integrating customer experience (CX), user experience (UX) and human-centered design principles into data security practices helps establish a secure environment that is both user-friendly and effective. At Maximus, we begin by understanding how users interact with agency data. Once we have a holistic view of those interactions, we can build robust security measures that augment, rather than impede, the user experience to enhance our customer's security postures.

(ctd.)




**Kynan Carver**  
Cybersecurity Lead,  
Maximus



By placing the user at the center of data security, we help our customers achieve:

1. Mitigated risk of human error: when security measures are perceived as frustrating or cumbersome, users are more prone to errors or seeking ways to bypass security, thus escalating the risk of data breaches.
2. Enhanced adoption of security practices: CX and UX play a pivotal role in fostering greater user compliance with security protocols, thus fortifying the overall security framework of the organization.
3. Early identification of threats: through vigilant monitoring of user behavior and feedback, organizations can swiftly detect and address potential security threats.
4. Improved security return on investment (ROI): by allocating resources toward user-centric security solutions, federal agencies will see heightened security and user compliance.

 **Good data security starts with knowing where your data is and how users are interacting with it. What are some of the first steps for federal agencies as they establish common data standards, inventory and data tagging to prepare for an effective data security strategy?**

**Carver** Federal agencies can enhance data security, compliance and operational efficiency through the integration of attribute-based access control (ABAC) with just-in-time (JIT) and just-enough access (JEA) principles. This strategy provides a foundation for advanced security measures, including AI-powered tools.

Agencies can start with a meticulous inventory and mapping of all data assets across systems and networks, encompassing structured, unstructured and sensitive data.

Data is then categorized based on sensitivity levels and regulatory requirements, which enables delineation of appropriate security controls for each data type.

**“When security measures are perceived as frustrating or cumbersome, users are more prone to errors or seek ways to bypass security, thus escalating the risk of data breaches.”**

**— Kynan Carver, Cybersecurity Lead, Maximus**



Mapping the flow of data illuminates its movement within the organization and across external systems, uncovering potential vulnerabilities and risk areas.

Agencies can also deploy uniform metadata tags to consistently categorize and describe the data, facilitating streamlined data retrieval and analysis.


Clear data ownership establishes responsibilities for each data asset, which promotes accountability and well-informed decision-making concerning data access and protection. Agencies can also use sensitivity labeling to affix pertinent labels to data based on sensitivity and compliance requirements, ensuring user understanding of handling procedures and access constraints.

Agencies should also define access permissions based on user, data and environmental attributes, such as job role, clearance level, location and time of day, aligning with ABAC principles.

In accordance with JIT principles, access privileges are granted when necessary and promptly revoked post-use. Simultaneously, JEA principles ensure users obtain the minimal access needed for their specific job functions.

Finally, swift detection of unauthorized access or anomalous behavior requires ongoing data monitoring and tracking to determine how, when and why data is accessed.

### **Why is a user-friendly data security strategy important for deploying emerging technologies, such as AI?**

**Carver** A robust, user-friendly data security strategy supports effective implementation of emerging technologies such as AI. Agencies can establish a secure environment for AI by giving prominence to usability, transparency and user education. This focus facilitates optimized, responsible AI use cases while mitigating associated risks. 



## FDA Eyes Global AI Partnerships to Safeguard Patient Data

The Center for Devices and Radiological Health director warns Congress of national security implications if the U.S. restricts AI development in medical settings threats.

BY MICHAELA SCOTT

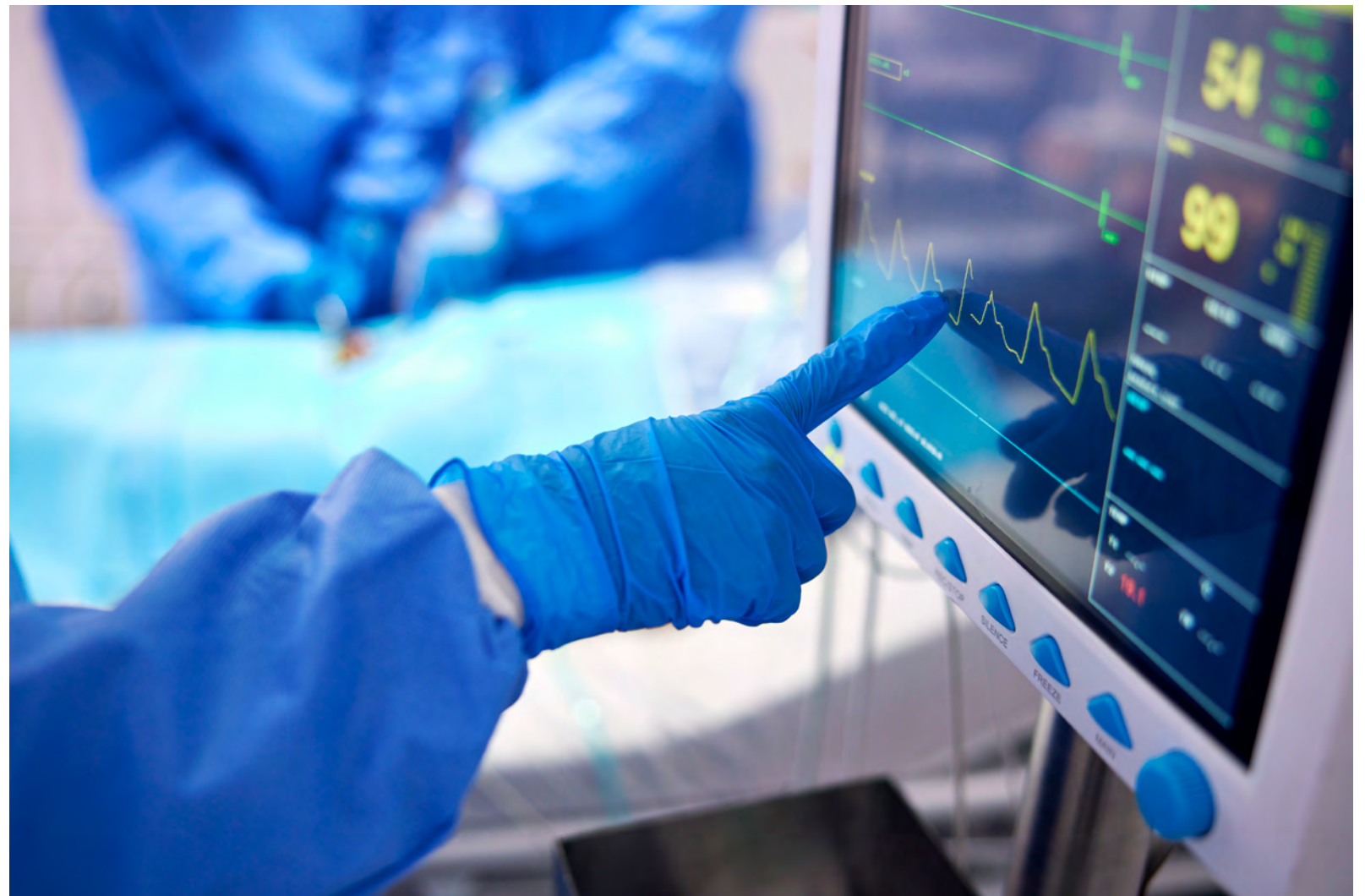
The Food and Drug Administration (FDA) is embracing artificial intelligence and working with international allies and partners to safeguard patient data and ensure the integrity of medical devices, agency experts said at a House hearing earlier this year.

Center for Devices and Radiological Health (CDRH) former Director Jeff Shuren said FDA has addressed cybersecurity vulnerabilities by working with industry partners to update cybersecurity requirements for medical devices in compliance with the Consolidated Appropriations Act of 2022.

Despite progress, CDRH identified that laboratory-developed tests — in vitro diagnostic products manufactured by laboratories and used in a single clinical laboratory — remain vulnerable to cybersecurity threats.

There is a critical need for greater oversight of these tests to ensure the innovation of safe and effective medical devices, Shuren added.

“We monitor several [vulnerabilities] at any given time, but there is still a weakness in laboratory developed tests,” Shuren said. “We have put out communications where we found vulnerabilities in platforms being used by non-labs and labs, but we only found out about it because it was used by non-labs. We made the manufacturer tell the labs, otherwise they would’ve



never known.”

CDRH is enhancing efforts to ensure that patches are provided to biomedical departments of hospitals and their service suppliers. Shuren said that working closely with industry partners is key to ensuring the

# Patrizia Cavazzoni

Director, Center for Drug Evaluation and Research (CDER), FDA



implementation of necessary security measures and timely patching vulnerabilities.

“This begins with designing devices in a way that allows them to be patchable,” Shuren said. “That’s what we work on with companies to assure that they’ve got the right measures in place. Then as we learn about problems and patches, we help yield that out.”

Center for Drug Evaluation and Research (CDER) Director Patrizia Cavazzoni emphasized the need for greater transparency within the supply chain to hold stakeholders accountable and address impending shortages in a timely manner.

“We would welcome having more authorities that would allow us to have greater transparency on the supply chain,” Cavazzoni said. “Greater transparency on the supply chain is certainly a tool that would really add to our limited toolbelt, so far.”

Shuren also noted that there are national security implications if the U.S. restricts AI development, emphasizing the need to embrace emerging technologies to remain the global leader in innovation. He said it’s important for FDA to facilitate AI development for medical systems in ways that are both safe and effective for patients.

He added that FDA is working with international partner governments to prevent duplication of requirements for companies that are marketing devices with AI.

“Much of our work for international harmonization on AI occurs in a group called the International Medical Device Regulators Forum,” Shuren said. “Typically in the AI space and digital health, when there are needs for changes in policies, we not only start here in the U.S., but we also take it to this group because all the countries are struggling with the same issues.”

Through efforts of fostering international collaboration, the group is now working on a globally harmonized policy regarding the lifecycle management approach for AI medical devices, Shuren said. (ctd.)

“We are trying to move [innovation] through as rapidly as we can while maintaining our gold standard,” added Center for Biologics Evaluation and Research Director Peter Marks. “We are always trying to do better, and that’s a commitment we have.”

Beyond collaboration with industry partners and international allies, Shuren

also emphasized the importance of government to help safely harness AI technologies and locate cybersecurity vulnerabilities.

“At the end of the day, if we want industry to be innovative and get innovations to people who need them, government has to be innovative too,” Shuren said. ✨

**“Greater transparency on the supply chain is certainly a tool that would really add to our limited tool belt.”**

**— Patrizia Cavazzoni, Director, Center for Drug Evaluation and Research (CDER), FDA**