

## 7 Cyber Areas That Deserve Your Attention

In the fast-changing and increasingly adversarial realm of cybersecurity, government IT leaders are racing to stand still. They're using limited resources to maintain their defenses and put out fires. And all of this is happening as agencies shift to a hybrid work environment, which requires fresh thinking about cyber strategies.

To understand how to best navigate this complex landscape, GovLoop recently hosted a roundtable, sponsored by HP Federal, that brought together cyber thought leaders from government and industry. They explored some key areas that call for the immediate attention of those tasked with ensuring the security of government data and systems. Here are takeaways from their discussion.

### ***Roundtable Participants***

**Dev Shenoy**, Principal Director of Microelectronics within the Office of the Undersecretary of Defense Research and Engineering, U.S. Defense Department

**Andrew Levitt**, Security Principal, HP Federal

**Jason Ralph**, Director, Security Operation Center, U.S. Department of Labor

**Tommy Gardner**, Chief Technology Officer, HP Federal

**Sean Starnes**, Chief Information Security Officer, Space CAMP, U.S. Air Force

**Angela Pompey**, CISO, Bureau of Labor Statistics, U.S. Department of Labor

## 1. Focus on Hardware Security

While there's been a lot of talk about ensuring the security of software, it would be a mistake to overlook hardware security, even down to the chip level. Semiconductors and microchips represent a significant potential area of vulnerability.

In any technology infrastructure, "it's really the semiconductors and microelectronics that enable those connected systems," said Dev Shenoy with the Department of Defense.

Bad actors can leverage hardware at the chip level to insert malicious code. "The hardware is critical. How do we ensure that when we design the hardware, manufacture it, assemble it, pack it and test it, that there is sufficient attention being paid to pre-empting those threats?" Shenoy said.

To that end, it's important to be skeptical of the global supply chain. "You've got suppliers in Asia, suppliers in China, that are obviously part of this ecosystem," he said. Anything coming through that supply chain should be viewed with a degree of wariness.

In government, there's been a lot of focus on requiring a software bill of materials: a complete list of the raw materials, components and instructions that inform the software. The same is needed on the hardware side. "Knowing what software you have doesn't help on a product if you don't know what hardware is there too," said Tommy Gardner with HP Federal.

## 2. Understand the Zero-Trust Mindset

Given federal mandates for agencies to adopt a zero-trust security posture, the topic is on everyone's radar. But IT leaders and other stakeholders may not appreciate the ramifications of this emerging approach.

Zero trust promises to impact all elements of the IT infrastructure, starting with the network. With remote work on the rise, "people are coming from anywhere and everywhere," said Jason Ralph of the Labor Department. "In this hybrid kind of environment, when they're coming from all these different locations, how do we make sure that we trust that person? Not only do we identify that device, but we want to identify that person, and we want to add more and stronger authentications."

Zero trust will require tools like a cloud access security broker, or CASB, for consistent enforcement of access control policies and other safeguards. Without such tools, "the sheer volume of it is overwhelming, [given] the number of endpoints you're dealing with," said Angela Pompey of the Labor Department.

And zero trust will demand a higher level of monitoring. "I have got to look at the logs, and make sure that I can identify those threats," Ralph said.



### 3. Protect People From Themselves

People will make mistakes. No matter how often you warn them, they'll still click on a well-disguised phishing link. Agencies need to find ways to protect people from themselves, and to safeguard the organization against the people.

"It's the people that you're trying to educate to not get tricked, not make mistakes. And people are fallible; they're going to get tricked, they're going to make mistakes," said Andrew Levitt with HP Federal. He added that it takes more than training to avert the risk here. It requires defense in depth "to have something that protects against things the users do," he said.

Gardner, for example, described a technique known as micro-virtualization, in which traffic is routed to a virtual environment and checked for security exploits, without ever touching the live system. "You can stop ransomware. You let people click anything they want to click and it won't do any damage," he said. "The malware stays in a virtual machine. It's isolated."

### 4. Be Intentional With Prioritization

The cyber threat is just too big: With all the risks out there, all the mandates agencies need to meet and limited resources at hand, it becomes especially important to organize one's efforts.

"Looking at zero trust in the executive order, and the sheer number of projects and solutions that we have to implement, how do we prioritize?" Pompey said.

"The solutions we already have in place, that is not a priority: We block a lot of things," she said. Instead, it makes sense to prioritize the implementation of new controls. But that effort comes with a trade-off. To test a new control, it's sometimes necessary to temporarily disable existing safeguards.

Ralph agreed. "A lot of times we do have to loosen up our controls because we have to allow them to be trained and tested ... for that unknown environment, for that unknown email that's going to maybe come in," he said. Even as IT teams establish their cyber priorities, they need to be thoughtful about how they bring new defenses to the fore.

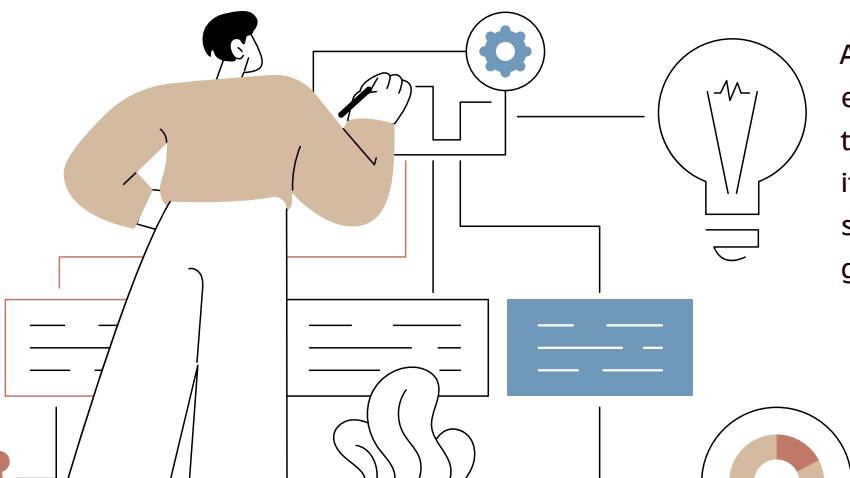
### 5. Create Nuanced Policies

The effort to create and enforce policy around IT use is never as simple and straightforward as one might like it to be. IT leaders can't control every aspect of how people engage with the tools.

"We can list out the things that we need to monitor. That is tangible," said Sean Starnes with Space CAMP. "But many issues come from a very dynamic landscape. We have something like 20 core government workers in our organization, and we have about 250 contractors. Contractors go in and out. We have no control over the machines."

To craft a nuanced policy that meets the need, Starnes takes a collaborative approach. "When we do policies, I put them out to the whole organization. I say, 'Hey, give me feedback on this. Is it going to break your workflow?'" he said. In balancing security and usability, that feedback ensures he gets "the best of both worlds."

Another way to simplify policy: "Treat all endpoints as compromised," he said. With this foundational zero-trust approach, it's easier to fine-tune policy to meet the specific needs of particular end-user groups.



## 6. Implement 'Secure by Design' Solutions

The Cybersecurity and Infrastructure Security Agency (CISA) defines "secure by design" products as those in which security is a core business requirement, not just a technical feature. "Secure by Design principles should be implemented during the design phase of a product's development lifecycle to dramatically reduce the number of exploitable flaws before they are introduced to the market for broad use or consumption," CISA states.

That same approach can guide the overall cybersecurity effort. In designing a nuclear reactor, "it's not only secure in your design, but it defaults to a secure place. If not, you're asking for trouble," Gardner said. "Same thing in the cyber world. You've got to have it where it's fail-safe."

CISA urges technology providers to bring this to life by taking ownership of customer security outcomes, embracing "radical transparency and accountability," and leading from the top. Federal IT teams can leverage these same strategies to ensure their IT ecosystems are intrinsically secure from the ground up.

## 7. Consider the Cyber Impacts of AI

Most of the news around artificial intelligence (AI) in government these days focuses on generative capabilities: AI can empower chatbots and create first drafts of reports. But AI potentially can have a big impact on cybersecurity efforts as well.

"We already have AI embedded in cyber tools," Pompey said. "Look at your endpoint detection and response: There's machine learning. There's the perimeter defense that has machine learning."

Federal agencies now need formal permission to leverage those capabilities. "We still need solid policy and guidance before we move forward with it," she said.

As that guidance emerges, AI-driven analytics will help identify anomalous behaviors. AI will support efforts to monitor network traffic, as well as capabilities such as security automation and response. All this, in turn, can help analysts save time and target their efforts, Ralph said.

The technology exists to support such advances. "Now you've got tools you never could have used in the '80s: The predictive capability is much, much higher," Gardner said. And the potential exists for even more profound enhancements.

With neural networks collapsing the space between digital logic and digital memory, we're seeing the rise of "new flavors of computing that I think can help AI do a lot better in the future," Shenoy said.

There's still much to be learned about the potential for computer intelligence to elevate cybersecurity efforts.

"We're in the early stages of unleashing what we can do with AI," Shenoy said. But with ever-advancing technologies and ever-expanding data sets for training the models, it's clear that AI is poised to have a significant impact on government efforts to secure data and systems against a range of increasingly sophisticated adversaries.

Learn more about HP's tools for government:  
[hp.com/us-en/solutions/government-it-solutions.html](https://hp.com/us-en/solutions/government-it-solutions.html)

