No Log Left Behind

HOW TO REACH OMB M-21-31 COMPLIANCE MODERNIZATION

DEVO

Across the public sector, IT leaders are adopting a zero-trust approach to securing their networks and tech stack. At the heart of zero trust is the motto: Assume breach. For many within security operations centers (SOCs), this means going through event logs to find a needle in the haystack. This was easier said than done, with varying standards across agencies and SOCs, until the **Office of Management and Budget's Memorandum 21-31**.

The 44-page OMB M-21-31 directs federal agencies to adopt a set of standards concerning event log management. Implementing the memorandum, however, **isn't without its challenges**. In "**Addressing OMB M-21-31,**" sponsored by Devo, federal and industry leaders came together to discuss the memorandum and what IT leaders can do to ensure no log is left behind.

Continue reading to learn more about OMB M-21-31. ↓

[01]

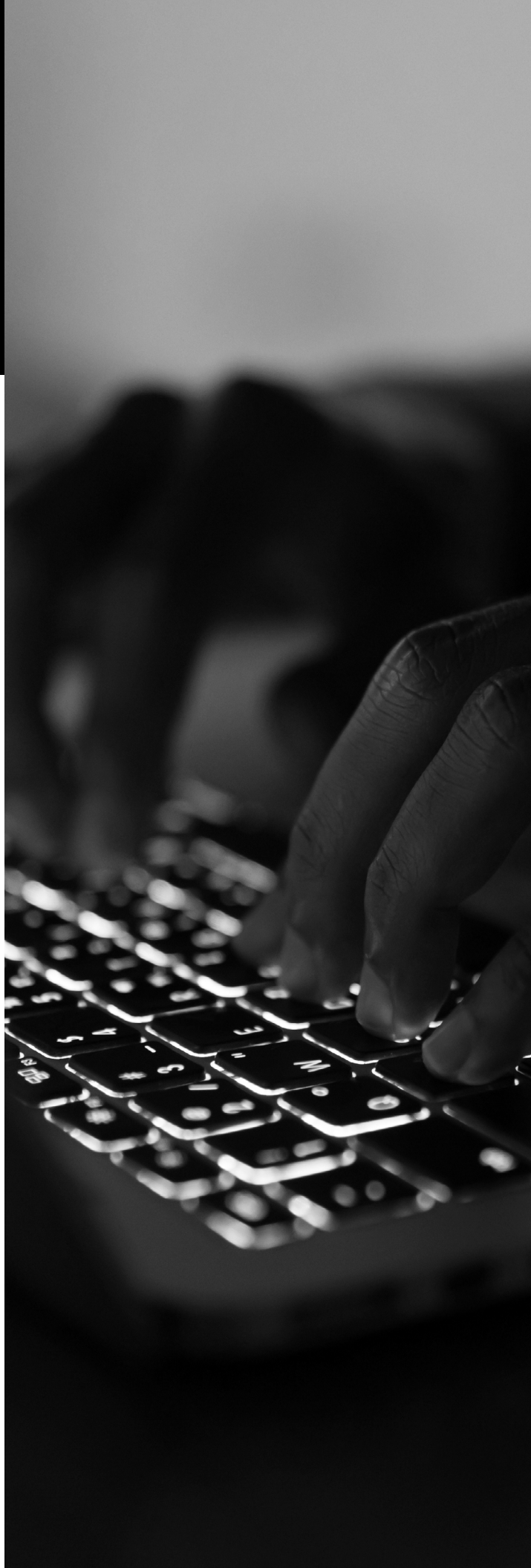
Be Proactive, Not Prescriptive With Timelines

Federal agencies range in size and complexity. Even the smallest organizations may have their own intricacies that make the adoption of federal mandates a monumental task.

Take, for example, the National Nuclear Security Administration. NNSA is a highly federated agency with multiple labs and sites. To adhere to the mandate, Deputy Chief Information Officer Steven McAndrews explains that his team had to start at the beginning.

“We had to start by doing the basics. Where are we at? What do we have? Not every site is at the same level,” he explains. “But we took the time to do a deep dive and figure out where we’re at and where we’re trying to go and working with the labs, plants and sites to make sure they’re choosing their own adventure, choosing their journey, as far as how to get there.”

McAndrews went on to explain that a prescriptive approach wouldn’t have worked, as resources vary depending on location — with some of NNSA’s labs being extremely rural — therefore, telling everyone to reach “x” capability by “x” date would’ve been an unreasonable request.



[02]

Work Together to Achieve EL3 Compliance

Reaching event logging tier 3 requires federal agencies to invest in automation and user behavior monitoring — two critical components in any zero trust architecture. For organizations that may not have the talent or resources to invest in EL3 requirements, creating a program to share the talent or resources they do have may end up helping advance compliance.

As IT leaders across the organization collaborate and share best practices, they are able to share outcomes and learn from each other about what is and isn't working. Compliance shouldn't be a check-the-box activity, says Don MacLean, chief cybersecurity technologist for TD Synnex Public Sector. Instead it should be a collaborative effort where all facets of the industry are working together in tandem.

"It's not going 'alright let's log this, let's log that,'" McAndrews says. "It's really looking at breaking out the stuff we have to log and then those additional capabilities and then really trying to figure out what's the best return on investment at the end of the day. We're going to all get there as a team, but what can we start in EL3 now that will pay dividends in the long run."

> It's not going 'alright let's log this, let's log that.' It's really looking at breaking out the stuff we have to log and then those additional capabilities and then really trying to figure out what's the best return on investment at the end of the day. We're going to all get there as a team, but what can we start in EL3 now that will pay dividends in the long run.

STEVEN MCANDREWS
Deputy Chief Information Officer
NNSA

[03]

Cultivate Talent by Building Bridges to Federal Employment

One of the biggest challenges for the public sector is recruiting and retaining top talent. The **Partnership for Public Service** states "about 83% of major federal departments and agencies struggle with staffing shortages and 63% report gaps in the knowledge and skills of their employees, according to a **2018 OPM report.**"

And since the publication of the OPM's Federal Workforce Priorities Report, talk in HR circles has shifted toward the "Great Resignation," all of which to say, talent is moving at a rapid pace.

Larkin Mize, cyber senior manager for Accenture Federal Services, confirms this by saying, "every company is realizing you've got to be out there and get that talent quickly."

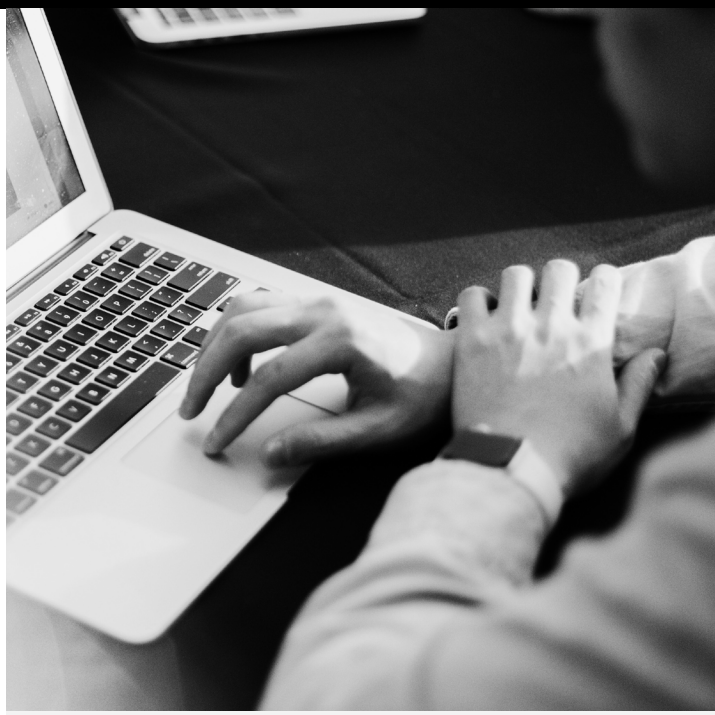
For the government, this presents a significant challenge, as the average time to onboard new talent is **98 days**. To cut down the time to onboard talent, agencies like the NNSA and others have established bridges to federal employment with programs like **Omni Technology Alliance**.

"We need more talented people. It's a supply-demand issue, so trying to cultivate that talent is important," McAndrews says.

DEVO

[04]

Gamify Learning About EL3 Components and Requirements



Threat actors move quickly. By the time students graduate with a degree in computer science or information technology, the methods and modes of attack will have changed. Across the industry, the speed with which cybersecurity moves is a complex issue — how do organizations ensure an applicant is up-to-date in terms of knowledge and tool sets? For MacLean, this is an area where the industry can step up.

"We need up-to-date training, and we need to make it engaging and fun," he explains.

For example, during the conversation, MacLean mentions that the British military conducts exercises where employees are locked in an "escape room" that requires swift problem-solving to mitigate threats to internet of things-enabled (IoT) devices in order to escape.

"The ones that work best — and people tend to roll their eyes or think this is trivial — [are] the ones that gamify things, that make it fun for people," MacLean explains. "But the thing is, people take this training, and they remember and implement it."

> "We need up-to-date training, and we need to make it engaging and fun."

DON MACLEAN
Chief Cybersecurity Technologist
TD Synnex Public Sector

[05]

Seek Out Interoperable Tools to Support Compliance

Standardization helps SOCs effectively navigate through the deluge of notifications. For threat hunters, the ability to analyze and connect related events across logs can help them better mitigate and contain potential threats to network security. Despite the benefits of standardization, agencies may find that tools or processes inhibit incident response efforts.

"A lot of tools sets out there are predefined to look at data that comes in a certain way, and when you start to get into big data lakes, they want to parse it their own way," Mize says. "Then you've got to figure out a tool that goes and [helps us] figure out how to look at it, which slows us down."

To support OMB M-21-31, government organizations should look for interoperable solutions that help them realize the full potential of their event logs and can ultimately help them move toward EL3 compliance.

> A lot of tools sets out there are predefined to look at data that comes in a certain way, and when you start to get into big data lakes, they want to parse it their own way. Then you've got to figure out a tool that goes and [helps us] figure out how to look at it, which slows us down.

LARKIN MIZE
Cyber Senior Manager
Accenture Federal Services

See how Devo can help your agency achieve EL3 compliance.

Read Now