DECS

8 Cybersecurity Trends and How You Should Respond A Roadmap for Federal Leaders

By Joanna Dempsey, Dave Howard, Keith McCloskey, Mike Zakrzewski, and Tony Zech

TABLE OF CONTENTS

Introduction	3
Trend 1: Cybersecurity Skills Gap	4
Trend 2: Cybersecurity Supply Chain Risk	. 5
Trend 3: The Importance of Trustworthy Data	. 6
Trend 4: API Attacks	7
Trend 5: Living Off the Land	. 8
Trend 6: Weaponizing Generative Al	. 9
Trend 7: Search Engine Optimization Poisoning	10
Trend 8: Threat Actor Misuse of Quantum Computing	11
Conclusion	12



INTRODUCTION

A Cyber Trends List Tailored for Federal Leaders

ith a quick search, you can find plenty of cybersecurity prediction lists online, and you'll see commonalities among them. But it can be hard to know which predictions to trust, which are most relevant to federal cyber leadership, and what you should do with the information.

Using our government and industry knowledge, we've tailored this list of cybersecurity trends and recommended responses to raise federal leaders' awareness of:

- Eight trends that are highly relevant to federal cybersecurity
- Ways to respond to and mitigate the threats, vulnerabilities, and other issues these trends present — from large-scale government responses to individual department and agency responses
- Readings and resources for additional learning

One high-level mitigation effort that applies to most of the eight trends we describe in this report is CISA's Secure by Design initiative. Secure by Design calls on manufacturers to develop products that are designed for security from the start and that come out of the box with secure configurations enabled by default.

We recently presented this information to a live audience: **our customers** at the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). This written report makes this same critical information available to all federal cyber and IT leaders.

"

API attacks have far-reaching impacts leading to data theft, service disruptions, and compromised security, eroding trust in digital services.

Read more about API attacks (Trend 4)



TREND 1 Cybersecurity Skills Gap

The demand for cybersecurity professionals will increase as agency operations are increasingly driven by technology, and the longstanding cybersecurity skills gap will continue to present staffing challenges. Factors contributing to this continuing challenge include:

The expanding digital landscape

A lack of diversity in cybersecurity^{1,2}

Retiring cyber professionals

- Fast technological advancement
- A competitive job market
- Worldwide digitization
- Increasingly complex cyber threats

Mitigation: Training, Diversity, and AI

From the national level to individual departments and agencies, our federal government can help mitigate the cyber skills gap through comprehensive training for new and current cyber professionals, workforce diversity programs, and automation and artificial intelligence (AI).

Federal leaders can:

Increase access to comprehensive cybersecurity training, with an expanded focus on future threats.

Continuously upskill and reskill the current cyber workforce.

Collaborate with academia to update curricula and offer specialized cyber programs.

Explore new, innovative ways that industry, government, and academia can shape and influence cybersecurity education to better suit employers' needs.

Build and enrich the talent pool by supporting workforce diversity efforts.

Invest in AI and automation to reduce toil and cognitive load, allow people to focus on the tasks at which they excel, and improve proactive defense against current and future threats.³

1. ISC2, 2023 ISC2 Cybersecurity Workforce Study 2. CISA, The Growing Threat to U.S. Critical Infrastructure 3. Work Economic Forum — Closing the Skills Gap whitepaper

Exploitable vulnerabilities are prevalent within most commercially available products, so the continued use of externally developed software, hardware, and data presents cyber supply chain risks.

With federal agencies relying heavily on commercially available information and communications technology (ICT)⁴ and 99% of businesses using at least one SaaS solution,⁵ supply chain risk will persist in both public and private sectors.

Mitigation: Follow CISA's Lead

To reduce supply chain risk, federal cyber leaders can leverage the work of authorities that have been established through federal legislation, executive orders, and federal acquisition regulations.⁷ Cyber leaders can develop and refine the guidance provided by:

- The CISA publication "Defending Against Software Supply Chain Attacks"⁸
- CISA's Secure by Design and Default initiatives and software bill of materials (SBOM) and supply chain risk management (C-SCRM)⁹ efforts

Cyber leaders can also collaborate with CISA's industry-recognized software security leaders to integrate **zero trust**, secure software engineering practices, and C-SCRM/SBOM tools into DevSecOps. Improved use of tools and processes in continuous integration and continuous delivery (CI/CD) pipelines (inventory, product supply chain/trusted repos, integrated security testing) can also help mitigate supply chain risk.

software and products.⁶ Notorious examples include:
SolarWinds code compromise (2020)
Apache Log4j vulnerability (2021)

Attackers can force-multiply their attacks by inserting and

disguising malware within legitimate and seemingly trustworthy

MOVEit vulnerability (2023)





^{4.} Government Accountability Office, GAO-21-171, INFORMATION TECHNOLOGY: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks 5. MarketsAndMarkets, Cloud Computing Market Growth 6. NSA, Software Supply Chain Attacks 7. Various legislation (SECURE Technology Act), Executive Orders (14017 – America's Supply Chains; 14028 – Improving Nation's Cybersecurity) have driven advances in federal regulations like CMMC and Federal Acquisition Security Council (FASC) Scorecard 8. Highlights NIST's Cyber Supply Chain Risk Management and Secure Software Development Frameworks 9. Example(s): GitBOM (https://www.youtube.com/watch?v=qcQFIv6pCSE w/ CISA's Aeva Black); OWASP CycloneDX (https://owasp.org/www-project-cyclonedx/); GovReady (now a part of RegScale, but has an opensource tool: https://github.com/GovReady)

The Importance of Trustworthy Data

As increasing amounts of system, personnel, and security data flood our databases, data trustworthiness will become an increasingly critical issue and making sense of this data at scale will become increasingly challenging.

Data feeds everything in an automated, AI-enabled world, and data that lacks accuracy, accessibility, or completeness produces untrustworthy results. Ensuring that we fuel our AI adoption and **attack surface management efforts** with clean, high-quality data is critical.

Mitigation: Leverage Your CDO's Work

By acquiring more high-quality, direct-from-source data and tying customer experiences into data governance, federal departments and agencies will be able to create more positive outcomes. Cyber leaders can leverage the work of department and agency chief data officers (CDOs). **CDOs identify and promote principles and best data practices such as:**

- Inventorying and tagging data
- Gaining a deeper understanding of data sets and how they are used to better inform your selection and protection of highvalue assets
- Aligning zero-trust-based authentication and authorization access to systems
- Improving controlled access and auditing of data





API Attacks

Because application programming interfaces (APIs) serve as vital connectors in the digital ecosystem, they are attractive targets for cybercriminals.¹⁰ Also, many modernization projects start by putting APIs in front of legacy systems and data without addressing necessary security controls.

API attacks have far-reaching impacts leading to data theft, service disruptions, and compromised security, eroding trust in digital services. These attacks can involve unauthorized access attempts, denial-of-service assaults, data theft, API key compromise, and more.

Mitigation: A Mix of Strategies and Solutions

Mitigating the unique security risks and vulnerabilities of APIs requires a blend of strategies and solutions. **Cyber leaders should:**

- Improve API governance (inventory, purpose, usage, data accessed, publishing, access controls).
- Strengthen authentication and authorization.
- Use API discovery tools.
- Deploy an API gateway.
- Deploy a web application firewall (WAF).
- Encrypt data.
- Use open authorization (OAuth) for controlling API access.
- Implement a zero trust strategy.¹¹



Cyber leaders should collaborate with data and system owners to understand the nature and context of the data being accessed; its create, read, update, and delete (CRUD) functions; the risks; and needed access, auditing, and reporting controls.

10. OWASP Foundation, API Security Project 11. WeLiveSecurity, All Eyes on APIs: Top 3 API Security Risks and How to Mitigate Them





TREND 5 Living Off the Land

Cyber threat actors will continue to use compromised credentials to gain access to systems and then use software, tools, and functions that normally exist on those systems to perform nefarious activities that leave no trace. This use of legitimate software, tools, and functions for malicious activity is called "living off the land."

Living off the land (LotL) attacks cannot be detected with traditional, signature-based cyber tools. Because the threat actors use tools and credentials already on systems and authorized to run, the malicious activities appear normal and benign.

Mitigation: Good Cyber Hygiene

The best defense against LotL attacks is to couple good cyber hygiene with improved host-level visibility and endpoint detection and remediation.

Cyber teams should leverage phishing-resistant multifactor authentication and zero-trust practices to ensure the right levels of authorization for common built-in tool usage. Behavioral-based anomaly detection will help to identify potential misuse of these common built-in tools.

Federal leaders can consult the CISA publication "Identifying and Mitigating Living Off the Land Techniques" (Feb, 2024) for extensive information about LotL threat detection and mitigations.

TREND 6 Weaponizing Generative Al

As all uses of generative AI (GAI) proliferate, so too will its nefarious use. Easily accessed and manipulated, GAI tools create content (e.g., video, voice, text) that closely mimics human-generated content.

Threat actors are using GAI in an increasing number of phishing, misinformation, disinformation, and identity theft schemes and will continue to harness the tool to spread false information, automate cyberattacks, and invade privacy. Such AI-driven threats have the potential to manipulate public opinion, undermine trust, and escalate cyber warfare.

Mitigation: Follow the CISA Roadmap

Federal cyber leaders and their teams should engage with relevant CISA decision support materials, risk management guides, and other educational efforts as they are developed. These are described in the **CISA Roadmap for Artificial Intelligence** ("Line of Effort 3").

While weaponized GAI is likely to increase the quantity of cybersecurity threats, it will not necessarily result in any new type of threat. As with LotL attacks, the best defense will be the continued upkeep of good cyber hygiene and defense. **Cyber leaders should focus on:**

- Al and data governance
- Employee education
- Strong authentication methods
- Al detection tools
- Content verification
- Robust IR plans
- Security and trust validation in AI design, development, training, testing, and production operation and usage





TREND 7

Search Engine Optimization Poisoning

Malicious actors will continue to exploit the trust users place in search engines to install malware on user devices and gain access to sensitive information.

Through search engine optimization (SEO) poisoning, threat actors manipulate search engine rankings to promote their malicious web content in search results. Using SEO tools such as keywords and metadata, threat actors increase their search rankings, so their content displays as a top search result. Unsuspecting users then navigate to these sites and fall victim to phishing, malware downloads, or scams.^{12, 13}

Mitigation: Eyes Peeled for Malicious URLs

With security training, cyber teams can raise user awareness of SEO poisoning. Departments and agencies should implement typosquatting¹⁴ detection procedures using digital risk monitoring tools. **They should also:**

- Leverage threat intelligence to detect malicious URLs.
- Upgrade software.
- Establish rigorous web filtering procedures.¹⁵

12. NJCCIC, SEO Poisoning: What Is in Your Search Results?13. McAfee, SEO Poisoning: A NewDrive-by Download Attack Vector14. A type of cybercrime that uses domain names that are slightlymisspelled versions of well-known websites.15. HC3 Analyst Note, SEO Poisoning

Threat Actor Misuse of Quantum Computing

Nation-state threat actors will continue to develop quantum computing technology as a future means of decrypting valuable, encrypted data belonging to rival nations, including the United States.

Scaled quantum computers can tackle complex problem sets by running thousands of scenarios simultaneously instead of sequentially. This can reduce problem resolution times from decades to days and render even the most complex encryption breakable.

While quantum computing technology capable of breaking public key encryption algorithms in the current standards does not yet exist, government and critical infrastructure entities ... must work together to prepare for a new post-quantum cryptographic standard to defend against future threats."

- From "Post-quantum Cryptography Initiative" (CISA.gov)



Mitigation: Learn and Prepare

"

As the decryption of data via quantum computing is a likely future threat and not a current threat, recommended mitigation now centers around education and preparation.

Chief information officers and cyber leaders can use **CISA resources** to plan and prepare for a transition to a new post-quantum cryptography standard, to be created by the National Institute of Standards and Technology (NIST). **General preparatory steps for organizations include:**

- Inventorying and prioritizing cryptographic assets (type, location, function, risk)
- Developing and implementing quantum-resistant encryption and algorithms
- Continuous monitoring of quantum computing developments and potential threats

CONCLUSION A Place to Start

The number of cybersecurity trends likely to overlap with the federal sector in the coming months and years is obviously more than eight. This tailored list is meant to give our customers and all federal cyber leaders a current, digestible introduction to a handful of pertinent trends and some recommended responses to those trends.

If you have questions about the information in this report or if you want to learn about how ECS leverages cyber threat intelligence, threat modelling practices, and tools such as ECS Argos PAI and ECS Pathfinder to proactively manage risk, please contact us.

Find the Authors of This Report on LinkedIn:

ECS is a leading information technology provider delivering solutions in cybersecurity, data and artificial intelligence, IT operations, enterprise transformation, and science and engineering. The company's highly skilled teams solve critical, complex challenges for customers across the U.S. public sector, defense, and commercial industries.



Joanna Dempsey in

Vice President, CISA Portfolio, Justice and Homeland Solutions



ECS maintains partnerships with leading cloud and cybersecurity technology providers and holds specialized certifications in their technologies.

Dave Howard in

Executive Director, Cyber Operations and Delivery, **Enterprise Managed Services**



Tony Zech

Director, Data & Artificial Intelligence



Mike Zakrzewski in

Senior Director, Cyber Technology, Justice and Homeland Solutions



Keith McCloskey in

Vice President and Chief Technology Officer, Justice and Homeland Solutions