PROTECTING AND ENSURING CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

National Intergovernmental Audit Forum Annual Conference

December 11, 2024

PROTECTING AND ENSURING CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

Moderator

Marisol Cruz Cain, CISSP, CIPP/US

Director, Information and Cybersecurity Team

U.S. Government Accountability Office

Panelist

Quinn Peralta, MCL, CISSP

IT Security Assistant Audit Manager

Office of the Washington State Auditor

Panelist

Kristen Bernard

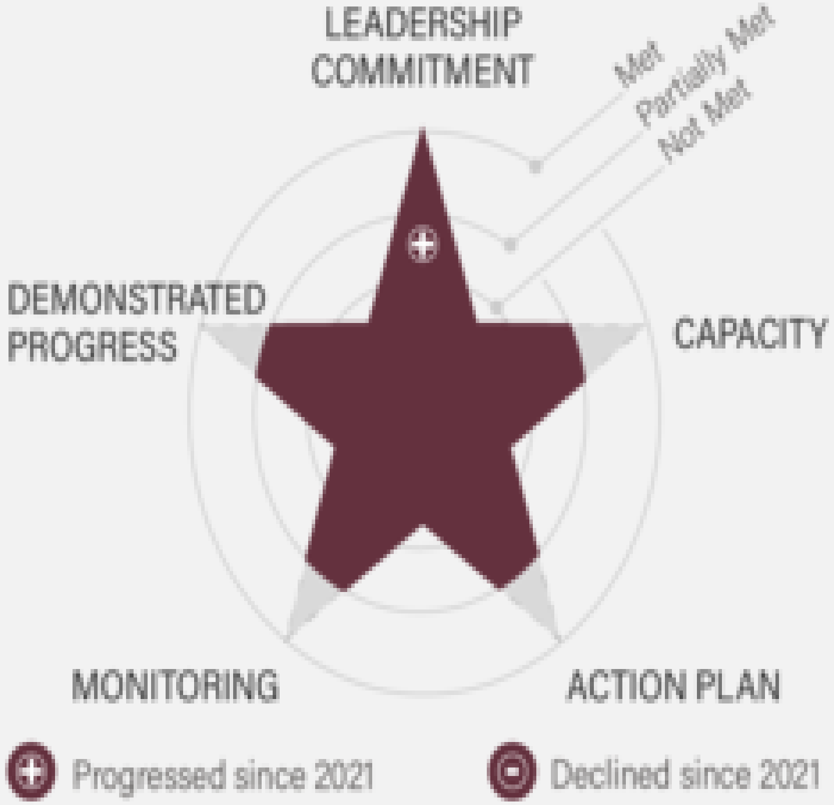
Deputy Inspector General for Audits

Department of Homeland Security

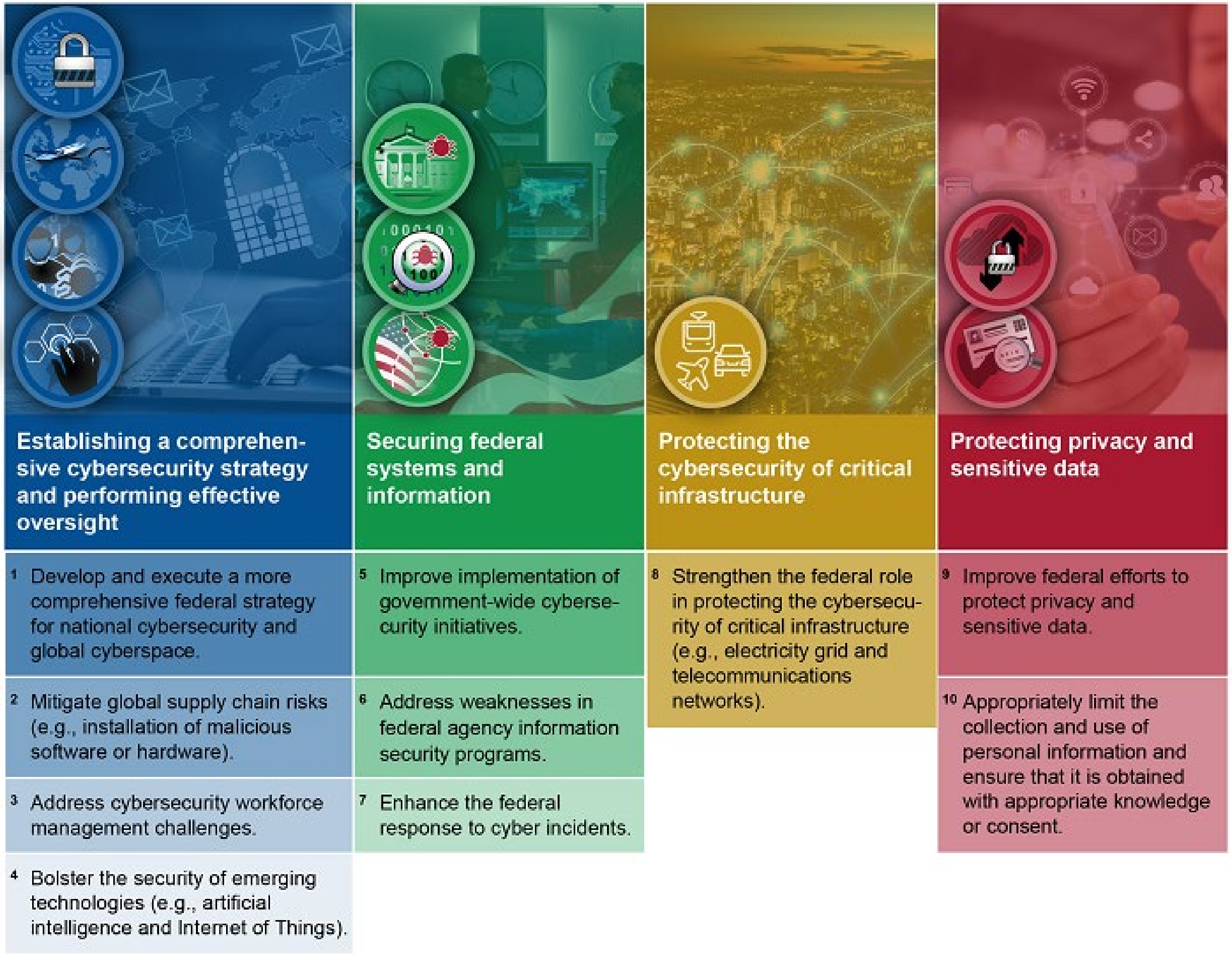
Office of Inspector General

GAO'S HIGH-RISK AREA: ENSURING THE CYBERSECURITY OF THE NATION

- In 1990, GAO began a program to report on government operations that we identified as "high risk."
- Information Security was added to the list in 1997 and has been updated with advancements in technology:
  - **2003 - critical infrastructure concerns**
  - 2015 - personally identifiable information
  - 2018 - comprehensive national strategy & oversight
- Federal and critical infrastructure IT systems and data are under increasing threat, which could result in serious harm to human safety, national security, the environment, and the economy.
- Federal agencies reported 32,211 information security incidents to the Department of Homeland Security's U.S. Computer Emergency Readiness Team in fiscal 2023.



FOUR MAJOR CYBERSECURITY CHALLENGES AND 10 ASSOCIATED CRITICAL ACTIONS



Establishing a comprehensive cybersecurity strategy and performing effective oversight

1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).

3 Address cybersecurity workforce management challenges.

4 Bolster the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

5 Improve implementation of government-wide cybersecurity initiatives.

6 Address weaknesses in federal agency information security programs.

7 Enhance the federal response to cyber incidents.

Protecting the cybersecurity of critical infrastructure

8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

Protecting privacy and sensitive data

9 Improve federal efforts to protect privacy and sensitive data.

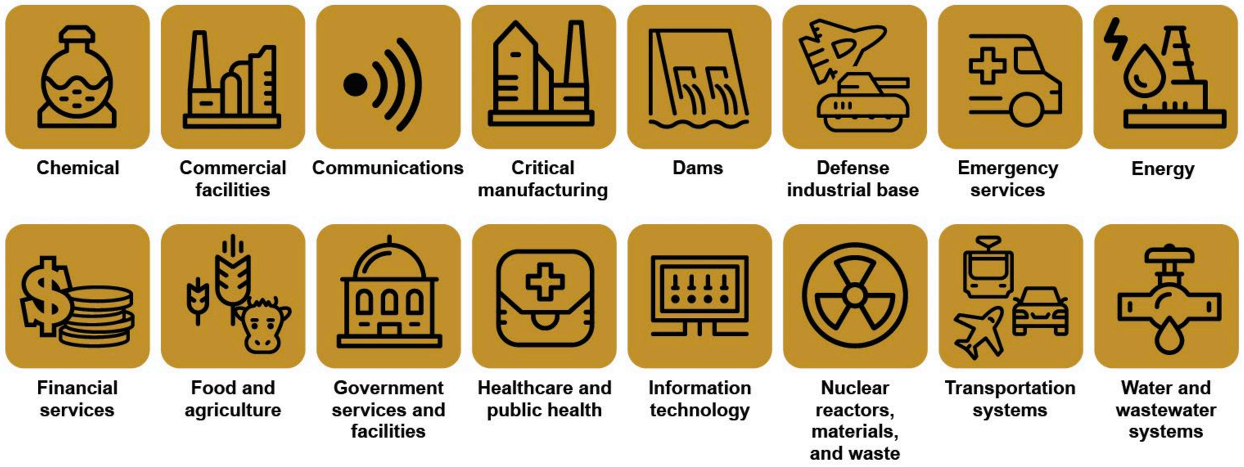
10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Sources: GAO (analysis and icons), Who is Danny/stock.adobe.com (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); https://www.whitehouse.gov (logo). | GAO-24-107231

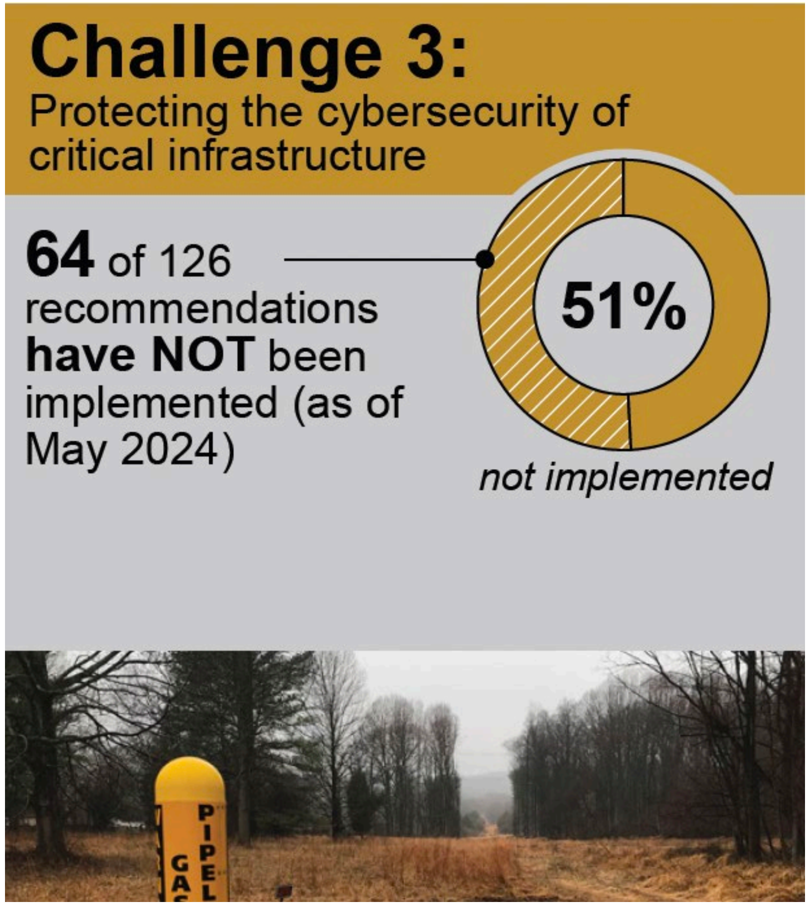
CHALLENGE #3: PROTECTING CYBER CRITICAL INFRASTRUCTURE

- The nation’s 16 critical infrastructure sectors provide the essential services that underpin American society.
- These sectors rely on electronic systems and data to support their missions, including operational technology, which consists of systems that interact with the physical environment.
- Attacks on these sectors continue to grow and could result in serious harm to human safety, national security, the environment, and the economy.

Figure 2: The 16 Critical Infrastructure Sectors



Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). | GAO-24-107231



Challenge 3:
Protecting the cybersecurity of critical infrastructure

64 of 126 recommendations **have NOT** been implemented (as of May 2024)

GAO'S HIGH-RISK AREA: ENSURING THE CYBERSECURITY OF THE NATION

In January 2024, GAO reported that the federal agencies responsible for the four critical infrastructure sectors that reported almost half of all ransomware attacks—critical manufacturing, energy, healthcare and public health, and transportation systems—had not determined the extent of their adoption of leading practices to address ransomware. (GAO-24-106221)

In March 2024, GAO identified challenges in collaboration between the Cybersecurity and Infrastructure Security Agency and other federal agencies with responsibilities for mitigating cyber risks to operational technology in their sectors. The challenges were related to ineffective information sharing and a lack of sharing processes. (GAO-24-106576)

In December 2023, GAO highlighted challenges identified by nonfederal entities in the healthcare sector in accessing federal support to address cybersecurity vulnerabilities in network-connected medical devices. (GAO-24-106683)

Moving the Needle on Security

Cybersecurity Services in Washington State

Quinn Peralta, IT Security Assistant Audit Manager

December 2024

PERFORMANCE AUDITING AND CYBERSECURITY

- I-900, passed by the voters in 2005, gave us authority to examine performance of any government in state
- Dedicated share of the state sales tax, which funds:
  - Performance audits
  - Cybersecurity audits
  - Center for Government Innovation

HOW WE CONDUCT AUDITS

Controls assessment

- Evaluates a government’s IT security controls against leading practices
- Conducted through a combination of interviews, documentation review (policies & procedures), evidence collection and limited technical testing

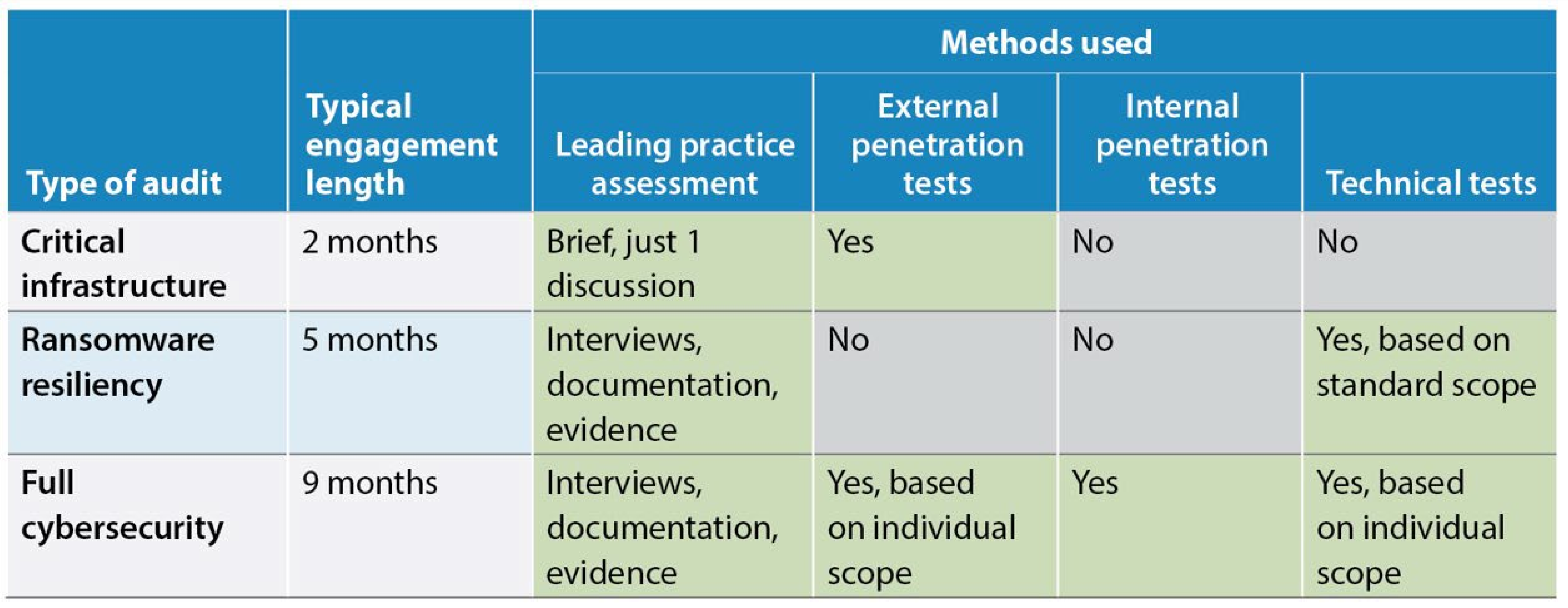
Penetration testing

- Uses a combination of automated and manual techniques to identify, and possibly exploit, vulnerabilities in an organization’s systems so the organization can learn about them and fix them accordingly

In-house technical testing

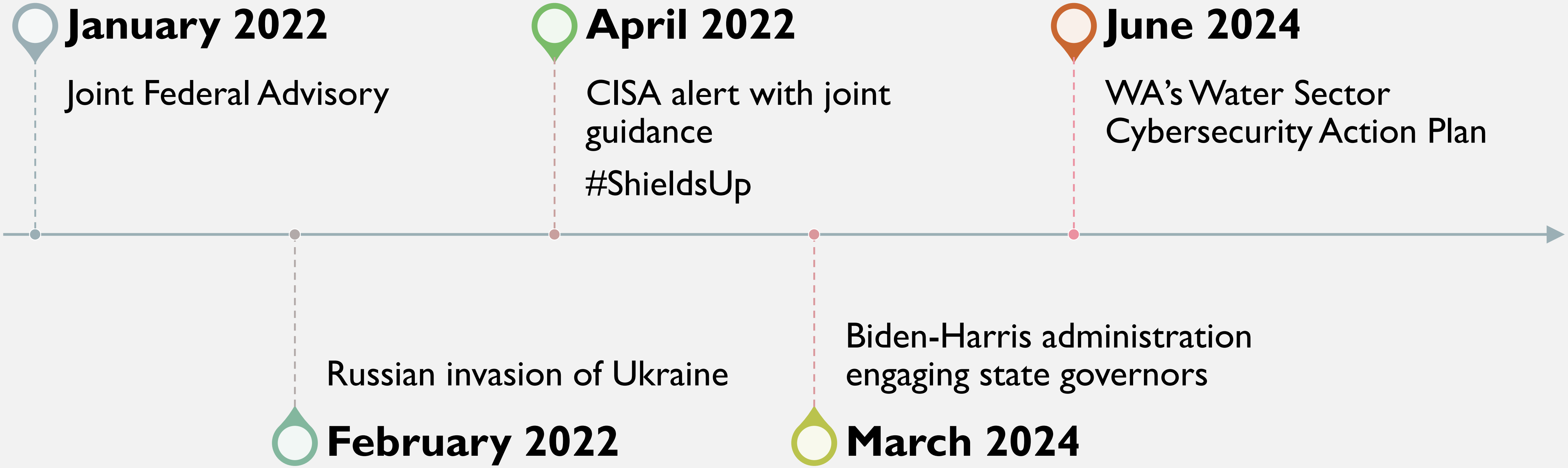
- Analyzes system vulnerabilities, configurations, or administrator privileges based on computerized scans of those systems

TYPES OF AUDITS – COMPARE & CONTRAST



		Methods used			
Type of audit	Typical engagement length	Leading practice assessment	External penetration tests	Internal penetration tests	Technical tests
Critical infrastructure	2 months	Brief, just 1 discussion	Yes	No	No
Ransomware resiliency	5 months	Interviews, documentation, evidence	No	No	Yes, based on standard scope
Full cybersecurity	9 months	Interviews, documentation, evidence	Yes, based on individual scope	Yes	Yes, based on individual scope

CRITICAL INFRASTRUCTURE AUDITS – HOW DID WE GET HERE?



January 2022

Joint Federal Advisory

February 2022

Russian invasion of Ukraine

April 2022

CISA alert with joint guidance

#ShieldsUp

March 2024

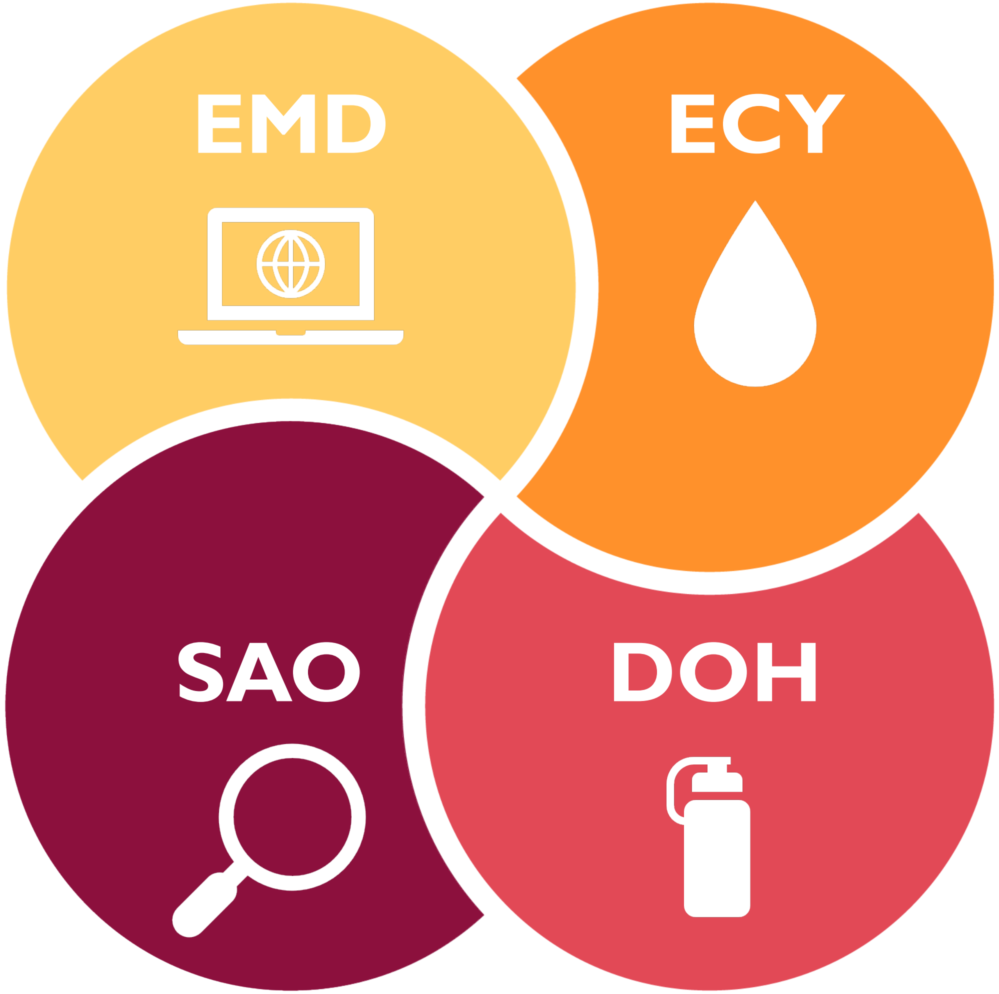
Biden-Harris administration engaging state governors

June 2024

WA's Water Sector Cybersecurity Action Plan

SAO'S ROLE IN WASHINGTON'S CYBERSECURITY ACTION PLAN

Cybersecurity & critical infrastructure SME; planning, exercise, training



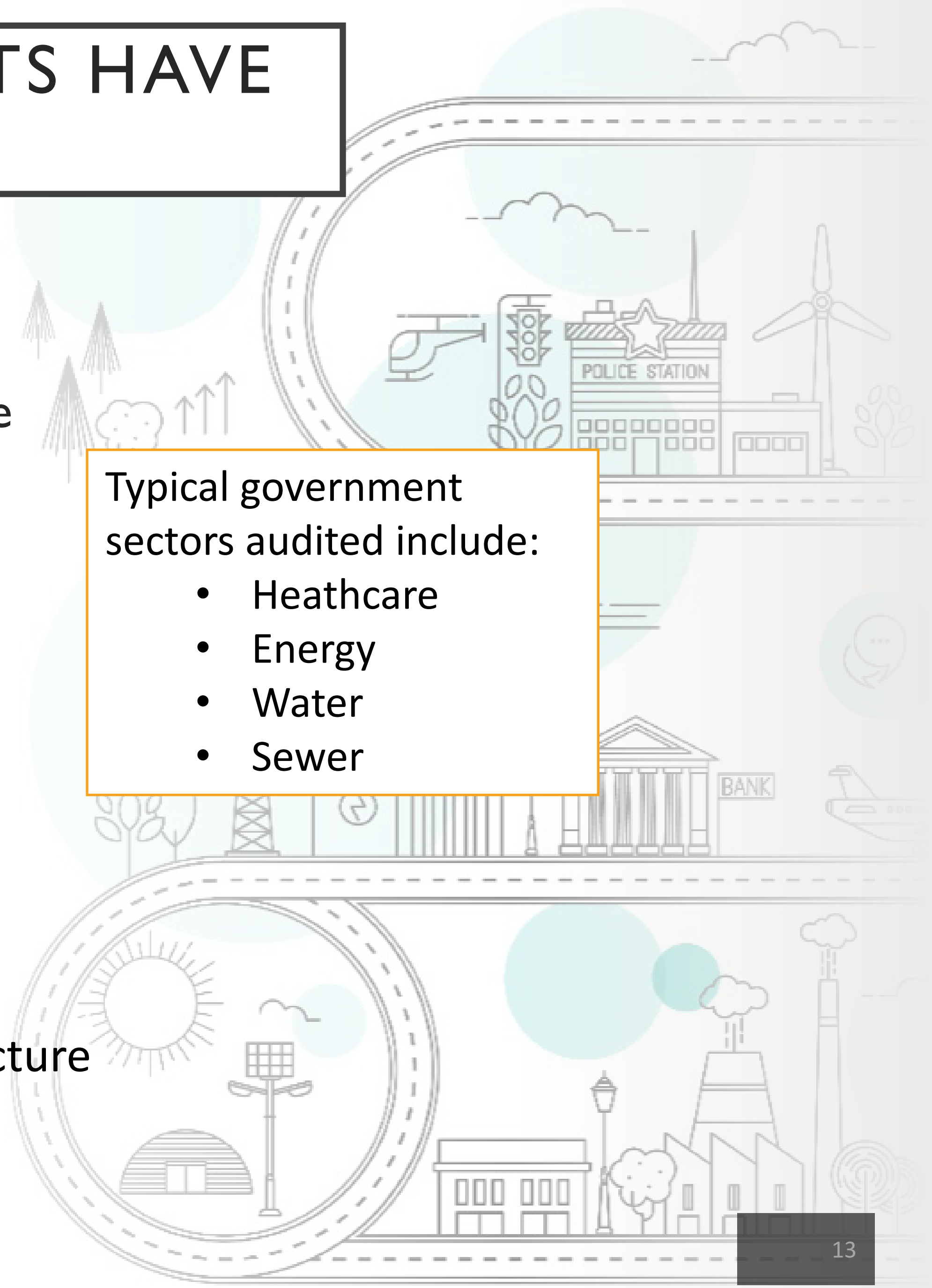
Wastewater state primacy agency; outreach & engagement

Cybersecurity & critical infrastructure audits

Drinking water state primacy agency; outreach & engagement

CRITICAL INFRASTRUCTURE AUDITS HAVE A SPECIAL FOCUS

- Responds to CISA's Shields Up campaign
- Focused on local governments providing critical infrastructure
- Interviews to identify specific areas for improvement
- Penetration testing of internet-facing assets



Typical government sectors audited include:

- Heathcare
- Energy
- Water
- Sewer

Audit question asks:

- Can selected local governments with critical infrastructure improve their external security posture?

EFFICIENT USE OF AUDIT RESOURCES PRODUCING USEFUL RESULTS

- Narrower scope resulted in:
  - ○ Less staff time needed at local government and SAO
  - ○ More audits completed more quickly
- Audited 51 local governments with critical infrastructure

Penetration testing identified over 300 vulnerabilities, with the following severity levels:

Severity					
Critical	**High**	Medium	Low	Informational & observations	**Total**
1	**51**	53	101	102	308

CONTACT INFORMATION

Quinn Peralta

IT Security Assistant Audit Manager

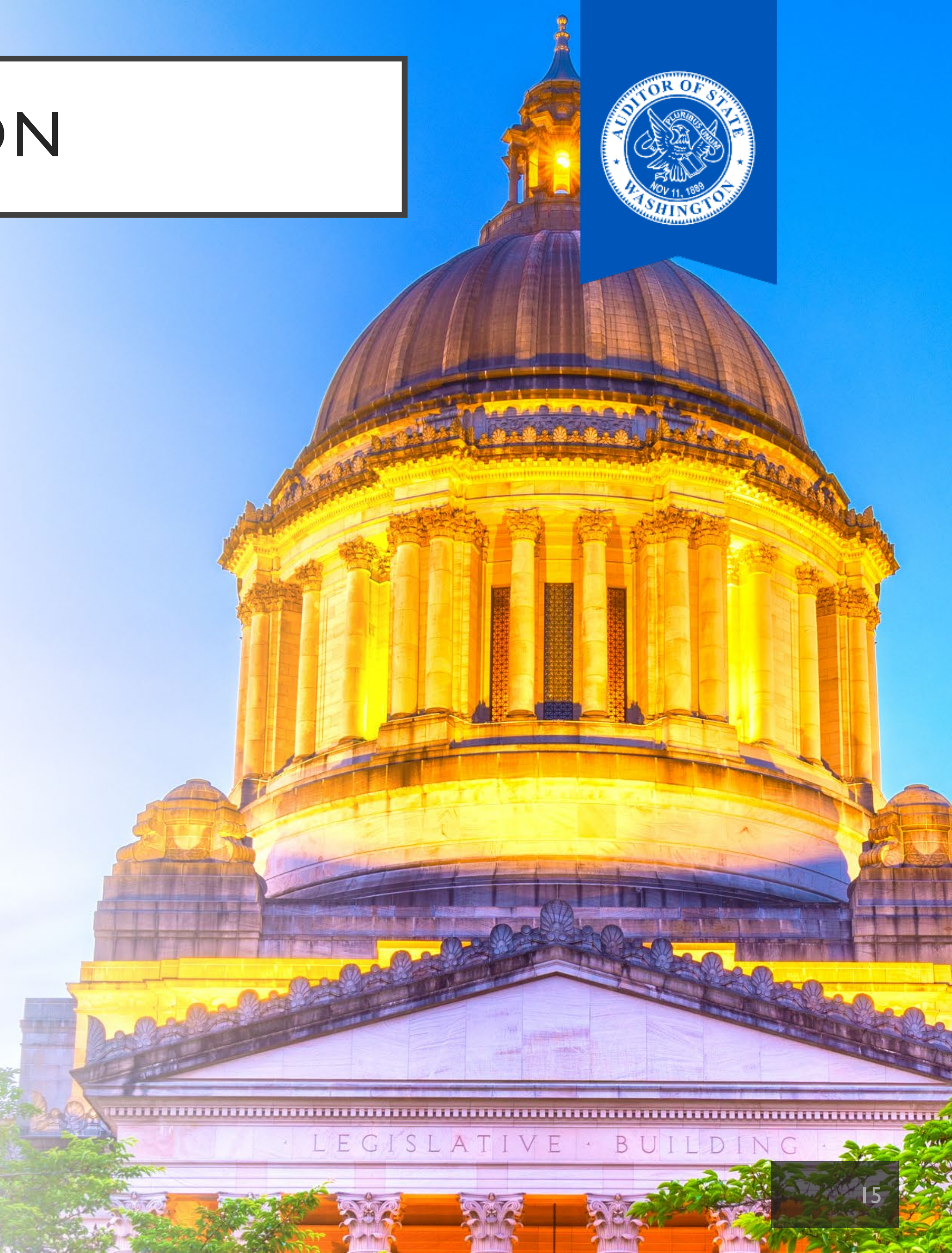
Quinn.Peralta@sao.wa.gov

Scott Frank

Director of Performance Audit

Scott.Frank@sao.wa.gov

Website: www.sao.wa.gov
X: @WAStateAuditor
Facebook: www.facebook.com/WaStateAuditorsOffice
LinkedIn: Washington State Auditor's Office



QUESTIONS?