Infrastructure Investment and Jobs Act cybersecurity

EY
Building a better working world

Infrastructure Investment and Jobs Act

On November 5, Congress passed the Infrastructure Investment and Jobs Act (IIJA) legislation that will provide $973b over five years from FY22 through FY26, including $550b in new investments across transportation, water, power and energy, environmental remediation, public lands, broadband and multiple approaches to improving resilience. The investment provides the opportunity to make substantial improvements at state, city and county levels. Realizing these benefits requires thoughtful strategy and engaged management of funding to prioritize, allocate and monitor.

Cyber investment

IIJA designates over **$2b in funding for cybersecurity** resiliency and innovation. The bill includes funds to reduce cyber vulnerabilities in public water systems and drinking/clean water technology. Additionally, the bill allocates funding to state and local via grant programs for cyber functions to include detecting and recovering from cyber threats and emergencies.

Cybersecurity in the IIJA

- **$1.31b for cyber resiliency for state and local**
  - Increase resiliency against cyber attacks on public and private networks at the state and local levels
  - Conduct research related to risk assessments and cyber vulnerability testing

- **$550m for grid infrastructure resiliency**
  - Detect and respond to cyber threats in rural and municipal utility systems
  - Develop advanced cybersecurity applications and technologies for the energy sector

- **$500m for clean/drinking water resiliency**
  - Increase resiliency to cyber threats and hazards in midsize and large drinking water systems
  - Study the state of technologies that could address cybersecurity vulnerabilities
  - Address rising threats to clean water infrastructure from climate change and cyber vulnerabilities

New and existing infrastructure faces increasing cyber and ransomware attacks that threaten public safety. With over $2b of funding dedicated to cybersecurity, water systems, electricity grids and other electrified infrastructure, agencies will need support protecting their systems from bad actors.

Cybersecurity program planning

Eligible entities applying for a grant under this plan to Department of Homeland Security Cybersecurity and Infrastructure Security Agency will need to submit a cybersecurity plan for review. Ernst & Young LLP (EY US) has deep cybersecurity strategy experience helping commercial and government clients develop a plan that captures security priorities, timelines and sequencing to address security gaps and mature the security posture of the organization. EY US has proven accelerators and National Institute of Standards and Technology-aligned cybersecurity frameworks to accelerate the development of cybersecurity road maps.

In addition, the EY Grants Accelerator can help entities applying for grants to organize the funding they receive.

Supply chain risk management

Agencies must address supply chain risk to effectively meet their mission. The EY supply chain risk management program helps agencies to identify, assess, and mitigate supplier risk across financial, cybersecurity, geopolitical, corruption and foreign interest risk lenses. Sophisticated data analytics can make these risks visible, help governments build resilience into supply chains and mitigate challenges.

How we can help

Operational technology/ critical infrastructure

Protecting one's critical infrastructure, such as water and electrical systems, is a crucial need today. Operational technology (OT) uses hardware, software, personnel and its activities, all focused on detecting or causing changes in industrial processes through direct monitoring and/or control of physical devices, to drive innovative changes in how organizations leverage technology to gain insights and capture market opportunity.

Ransomware readiness and resilience

Our approach is driven by threat intelligence to create outcomes across multiple processes and organizations so that they are enhanced to protect your organization from ransomware attacks. Our R^3 service offering (NGSO&R) protects your organization by understanding your unique risks and enumerating them for rapid remediation; enhancing your capability to identify, protect, detect, respond and recover from a ransomware event; and demonstrating secure and consistent business operations for your enterprise and its stakeholders.

Case studies

1. EY teams have helped and currently support multiple **state agencies** with assessing their cybersecurity maturity and developing a prioritized cybersecurity plan to address security risks and mature security posture.

2. We are currently supporting a **large federal organization** with the creation of a cyber-supply chain risk management program to identify and mitigate potential risks associated with the utilization of suppliers. The program is now fully operational and was recently granted the authority to be offered as a service to external federal agencies.

3. The EY team is currently building an OT cybersecurity program for a **large federal transportation organization.** Utilizing both commercial and federal leading practices, we are helping to identify, assess and mitigate OT cybersecurity risks while evolving the program to meet changing threats.

4. A **large state transportation agency** engaged EY US for a ransomware assessment to improve cyber resilience. In addition, the EY team evaluated the security tool suite by simulating attack scenarios on selected systems to determine whether the security tools prevented, alerted or logged the attack.

Sample of EY cybersecurity services related to IIJA

- Cyber program planning and grant management
- Operational technology cyber program creation and transformation/critical infrastructure
- Supply chain risk management
- Ransomware resilience and NGSO&R