U.S. Department
of Transportation

Implementing Cybersecurity Actions into Transportation Infrastructure Projects

Office Of The Secretary

Bipartisan Infrastructure Law and Inflation Reduction Act

Federal Register / Vol. 88, No. 210 / Wednesday, November 1, 2023 / Notices 75083

Critical Infrastructure Security, Cyber Security and Resilience: It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats, consistent with Presidential Policy Directive 21—Critical Infrastructure Security and Resilience and the National Security Presidential Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. Each applicant selected for Federal funding under this notice must demonstrate, prior to the signing of the grant agreement, effort to consider and address physical and cyber security risks relevant to the transportation mode and type and scale of the project. Projects that have not appropriately considered and addressed physical and cyber security and resilience in their planning, design, and project oversight, as determined by the Department and the Department of Homeland Security, will be required to do so before receiving funds for construction.

- The Bipartisan Infrastructure Law (BIL) and the Inflation Reduction Act (IRA) have created the opportunity for states, territories, Tribes, and local governments to make a once-in-a-generation investment in infrastructure
- As you read the Notice of Funding Opportunity, you may come across a paragraph called “Critical Infrastructure Security and Resilience (CISR)”

CISR in DOT Notice of Funding Opportunity (NOFO) Announcements

U.S. Department of Transportation

Critical Infrastructure Security and Resilience

"It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against all hazards, including physical and cyber risks, consistent with Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience, and the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. Each applicant selected for Federal funding must demonstrate, prior to the signing of the grant agreement, effort to consider and address physical and cyber security risks relevant to the transportation mode and type and scale of the project. Projects that have not appropriately considered and addressed physical and cyber security and resilience in their planning, design, and project oversight, as determined by the Department and the Department of Homeland Security, will be required to do so before receiving funds."

Questions You May Be Asking

- Why is the Federal Government asking me to consider cyber risks in my project?
- Will this apply to my project?
- What exactly will I have to do to meet the requirements?
- Can the Federal Government give me some guidance to make sure I do it correctly?

Questions You May Be Asking: Why is this necessary?

Why is the Federal Government asking me to consider cyber risks in my project?

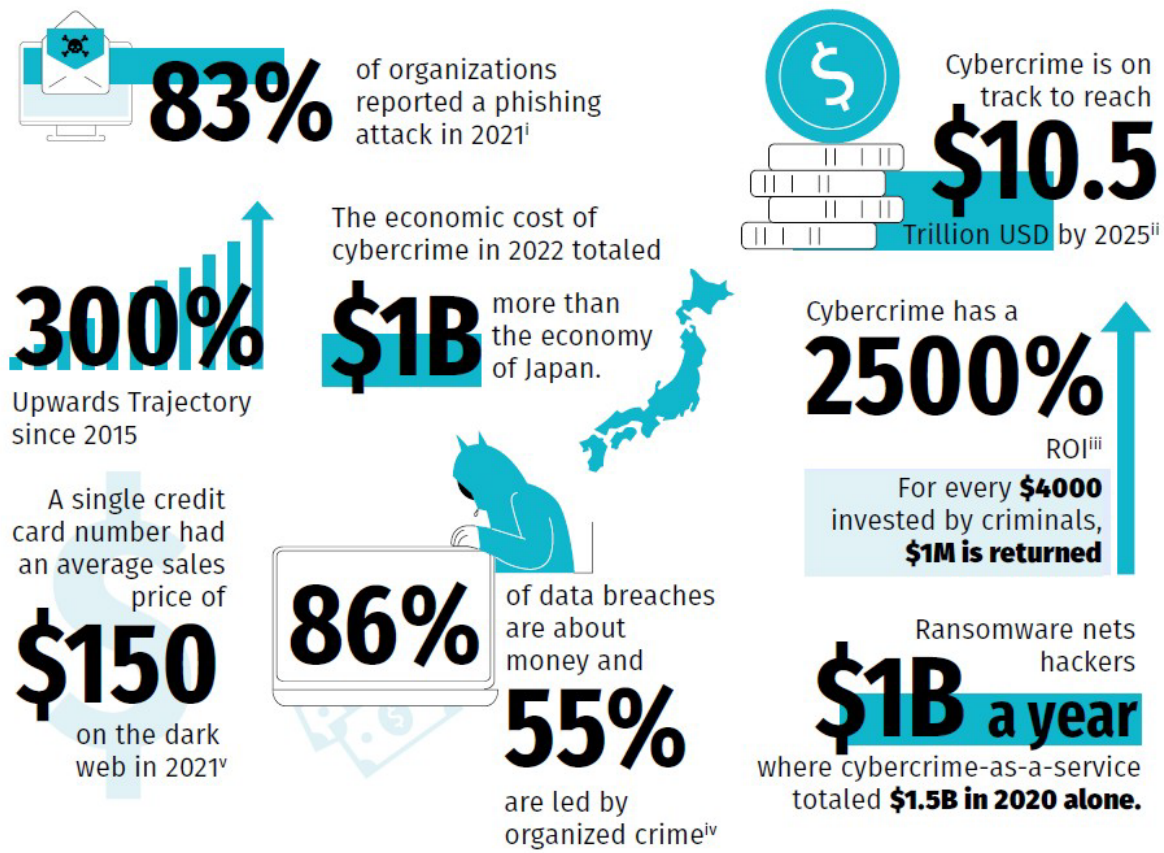
Why Target Critical Infrastructure?

The ROI of Cybercrime

Where there is profit, there is opportunity.

The economic impact of cybercrime has tripled in the past decade. No longer the hacker in a hoodie, today's threat actor is a professional. Structured and top line focused, organized cybercriminals act as an enterprise – following the same rules of finance as their targets.

"We can no longer separate cybersecurity from safety."
- Secretary Pete Buttigieg, June 12, 2023



Infographic source: The ROI of Cybercrime (www.sans.org)

Why Target *Transportation* Critical Infrastructure?

Transportation Supports Multiple Other Infrastructure Sectors

- Allows each geographic area to produce whatever it does best and then trade its product with others
- Speedy modes of transportation allow perishable goods to be distributed to wider market areas
- Transportation allows workers to reach their job sites

Transportation is Vital to the U.S. Economy and National Security

- Transportation accounted for 8.4% of U.S. GDP in 2021
- Transportation and transportation-related industries employed 14.9 million people in 2021, representing 10.2% of the U.S. labor force
- Thirty-eight percent of U.S. gross output in 2020, equivalent to $12.44 trillion, depended on the Nation's Transportation and Logistics sector, which itself contributed an output of $565 billion
- In 2020, over 17 billion tons of domestic freight worth $14.5 trillion moved through about $7 trillion of assets consisting of ports, highways, rail systems, airports, and pipelines

Source: 2022 DOT Bureau of Transportation Statistics

And They're Already Trying

Russia

- Russia remains a highly sophisticated cyber threat with the ***capability to disrupt or damage critical infrastructure***
- Intelligence indicates Russian cyber actors pursue cyberattack options against transportation and other targets

China

- The US Government assesses China presents the broadest, most active, and persistent cyber threat to US Government and private sector networks
- China's military doctrine emphasizes conducting cyber operations to preempt an adversary by paralyzing its information systems
- If China believed that conflict with the United States was imminent, ***China could attempt disruptive cyberattacks against US transportation infrastructure***

Iran

- Iran has a history of leveraging offensive cyber operations and other asymmetric tactics to pursue national interests
- Since at least 2018, Iranian cyber actors have targeted a range of US critical infrastructure sectors, ***including transportation and oil and natural gas***, to gain access to systems before follow-on operations

Questions You May Be Asking: Project Applicability

Will this apply to my project?

Will This Apply to My Project?

- The Risk of your project will determine whether cybersecurity requirements will be applied
- If there is little or no Information Technology content in your project scope, or you already have a cybersecurity program in place that meets DOT expectations or fulfills the requirements of another Federal agency, this will result in a “Low” cybersecurity risk determination
  - *No further action needed*
- If there is Information Technology content present in your project scope, this will result in an “Elevated” cybersecurity risk determination, and this will be addressed in either guidance or requirements to use **DOT’s BIL Cybersecurity Approach**
  - *Guidance will be provided for Formula/Entitlement grants*
  - *Requirements will be applied for Discretionary/Competitive grants*

Questions You May Be Asking: Meeting Requirements

What exactly will I have to do to meet the requirements?

What Exactly Will I Have To Do?

- Implement **DOT's BIL Cybersecurity Approach**

    1. Designate a Cybersecurity POC
    2. Develop a Cyber Incident Response Plan
    3. Develop a Cyber Incident Reporting Plan
    4. Complete a Cybersecurity Self-Assessment within two years of the beginning of the period of performance for the grant

Requirements may be adjusted to prevent creating redundant, overlapping, or conflicting requirements with existing requirements from TSA, US Coast Guard, or other government agencies

Questions You May Be Asking: Where is the Guidance

Can the Federal Government give me some guidance to make sure I do it correctly?

Designate a Cybersecurity POC

- Identify the individual who can be contacted by DOT or CISA and can answer questions about the organization's implementation of **DOT's BIL Cybersecurity Approach**
- No specific position or title requirements
- No training requirements prior to designation, but a commitment to complete introductory cybersecurity training within 1 year (see additional resources for example training)

Develop a Cybersecurity Incident Response Plan

- The Incident Response Plan should:
  - Identify an Incident Manager (IM) – this person will manage communication flows, update stakeholders, and delegate tasks
  - List the steps necessary to isolate the infected system(s) from uninfected systems, networks, and devices
  - List the steps necessary to fully restore any capabilities or services that are impaired during a cyber event
- Resources and Templates are available on the DOT Office of Sector Cyber Coordination website

Develop a Cybersecurity Incident Reporting Plan

- What is a "Cybersecurity Incident?"
  - An attempt to gain unauthorized access to a system or its data; or
  - An unwanted disruption or denial of service; or
  - Abuse or misuse of a system or data in violation of policy
- Develop a short plan that describes who to contact to report a cybersecurity incident or Internet crime
  - Report to CISA: www.cisa.gov/report ***OR*** report@cisa.gov **OR** (888) 282-0870
  - Their website has an intake form where you can provide details about the incident:
    - An incident description, including when the incident started and when it was detected
    - Information about the impact the incident has had on your organization, and whether the confidentiality, integrity, or availability of your organizations systems were potentially compromised
  - You can also contact your local FBI Field Office (www.fbi.gov/contact-us/field-offices) to report Internet crime

Conduct a Cybersecurity Self-Assessment

- DOT does not require you to use a specific assessment process, and there are several publicly available self-assessments you can find on the Internet. The following three assessments are highly recommended:
  1. Cyber Assessment Tool for Transit (CATT)
     While this assessment tool is geared toward transit agencies, it is closely based on an existing tool developed by CISA called the Cyber Resilience Review (CRR), which is not specific to any one mode of transportation or infrastructure sector. Your organization will answer a set of questions, and the tool will produce a report that summarizes gaps and recommended actions to close those gaps.
  2. CISA Cybersecurity Performance Goals (CPGs) Checklist
     CISA's CPGs are a common set of protections that organizations should implement to reduce cybersecurity risks. The CPG Checklist can be used to prioritize and track your organization's implementation of the CISA CPGs and identify areas of improvement.
  3. TSA Cybersecurity Vulnerability Assessment
     TSA has developed a Cybersecurity Self-Assessment Checklist which utilizes the functions and categories found in the NIST Cybersecurity Framework. It is a straightforward questionnaire, and your answers will help determine your current cybersecurity posture and where improvements can be targeted.
- Industry trade groups also publish self-assessment tools, and additional resources can be found on the DOT Office of Sector Cyber Coordination website

Need More Help?

- Please keep in mind that DOT does not provide dedicated grant funding to support these cybersecurity actions
- If you are looking for additional help implementing these actions, please refer to the resources located on the DOT OCIO Office of Sector Cyber Coordination website
- If you have other questions, please contact the DOT Office of Sector Cyber Coordination at:

DOT-Sector-Cyber@dot.gov

Certificate of Completion

This certifies that

<NAME>

Has successfully completed

Implementing Cybersecurity Actions into Transportation Critical Infrastructure Projects

Completed on <Date>

Length (in hours): 0.50