U.S. DEPARTMENT OF TRANSPORTATION

Federal Highway Administration

Order

Subject
FHWA Cybersecurity Program (CSP)

Classification Code	Date	OPI
1640.3	April 17, 2014	HAIS-30

Par.

1. **What is the purpose of this directive?** This directive establishes the Federal Highway Administration's (FHWA's) Cybersecurity Program (CSP) and its policy.

2. **Is this a new FHWA directive?** Yes, this is a new directive.

3. **What is the background of this directive?**

   a. Federal agency information has become increasingly under attack by sophisticated cyber threats originating in unfriendly nation-states, international criminal syndicates, and even within the United States. As a result, FHWA, under the direction of the U.S. Department of Transportation (DOT), must be prepared to manage these threats in a manner that minimizes their negative impact on FHWA information and its mission.

   b. DOT Order 1351.37, Departmental Cybersecurity Policy, requires that all DOT "Components" (Operating Administrations) must implement and comply with the policies in the Order to ensure:

      (1) The protection of DOT information systems and the sensitive data they contain from unauthorized access, use, disclosure, disruption, modification, or destruction from threats that can impact confidentiality, integrity, and availability of the information, information technology services, and communications; and

(2) Compliance with mandatory security-related laws, regulations, and guidance.

4. **What is the scope of this directive?** This directive applies to:

   a. All FHWA employees, contractors, subcontractors, and other users of FHWA information and information systems; and

   b. Information and information systems that support FHWA's operations and assets, including those provided or managed by another Federal agency, a contractor, or other source.

5. **What authorities were used in writing this directive?**

   a. DOT Order 1351.37, Departmental Cybersecurity Policy, Chief Information Officer Policy (CIOP) Chapter 37, which implements the requirements specified in the Federal Information Security Act (FISMA) of 2002 and related laws, regulations, and other mandatory guidance and standards related to information security, information assurance, and network security.

   b. DOT Departmental Cybersecurity Compendium, which specifies Departmental policy, guidance, and standards necessary to implement the requirements outlined in DOT Order 1351.37.

   c. DOT Security Authorization & Continuous Monitoring Performance Guide, which establishes the Departmental processes, procedures, and standards for implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework to support the initial security authorization, reauthorization, and continuous monitoring of security of DOT information systems.

6. **What is the definition of cybersecurity?** Cybersecurity is the performance of information security, network security, and information assurance to protect information systems and information infrastructure along with the sensitive data they contain from unauthorized access, use, disclosure, disruption, modification, or destruction from threats that can impact confidentiality, integrity, and availability of the information, information technology services, and communications (DOT Order 1351.37, Appendix B, Glossary).

7. **What is the FHWA policy concerning cybersecurity?**

   a. The FHWA adopts and will implement the policy and guidance in the following:

      (1) **DOT Order 1351.37, Departmental Cybersecurity Policy**. This Order is the foundational policy document within DOT which establishes the DOT CSP. It provides high-level policy and

establishes roles and associated responsibilities for implementing cybersecurity across the Department.

(2) **Departmental Cybersecurity Compendium**. This Compendium is a collection of supplemental cybersecurity policies as well as standards, procedures, and other guidance necessary to ensure the Department meets governmentwide cybersecurity requirements and to establish Departmentwide standardized processes. The Compendium contains policy which has the full force of the DOT Order 1351.37. The DOT Order grants the authority to the DOT Chief Information Officer to issue and update policy via the Compendium.

b. This directive also establishes the FHWA CSP as documented in the FHWA CSP Handbook. The FHWA CSP:

(1) Ensures FHWA's compliance with DOT Order 1351.37 and its associated Compendium;

(2) Ensures consistency throughout FHWA in applying the policies, processes, procedures, and standards of the DOT CSP; and

(3) Identifies FHWA specific cybersecurity policies, processes, procedures, and standards for those cybersecurity areas where DOT has requested definition at the DOT Component level or where FHWA as a DOT Component is allowed to tailor the DOT CSP to provided adequate protection for FHWA information systems and the sensitive data they contain from unauthorized access, use, disclosure, disruption, modification, or destruction.

8. **What are the roles and responsibilities for the FHWA CSP?** All FHWA employees, contractors, and subcontractors are to follow the specific cybersecurity responsibilities in DOT Order 1351.37. The FHWA CSP Handbook provides clarifications pertaining to FHWA for the roles and responsibilities listed within DOT Order 1351.37.

9. **Where can I obtain additional information in carrying out this directive?** For additional information on FHWA's CSP, contact the Office of Information Technology Services IT Policy Team.

Gregory G. Nadeau
Deputy Administrator