# Improving the Resilience of National Postal and Related Transportation Critical Infrastructure

**Julia Allen, Pamela Curtia, Dr. Nader Mehravari**
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

**Gregory Crabb**
U.S. Postal Inspection Service
475 L'Enfant Plaza SW
Washington, DC 20260-3101

***Abstract*— The United States Postal Inspection Service (USPIS) has collaborated with the CERT® Program at Carnegie Mellon University's Software Engineering Institute (SEI) to improve the security and resilience of selected United States Postal Service (USPS) products and services. Developing and implementing measurable methodologies for improving the security and resilience of a national postal critical infrastructure sub-sector directly contribute to protecting public and postal employees, assets, and revenues. Such methodologies also contribute to the security and resilience of other modes of transport and to the protection of the global supply chain.**

**Outcomes of this collaboration demonstrate that the use of modern resilience management frameworks and the associated techniques enable a structured, repeatable, and integrated approach for owners, operators, and regulators of critical transportation infrastructures and subsectors. This approach enables more effective planning, assessment, management, and sustainment of transportation products and services to ensure that they meet all required security, safety, and resilience needs, particularly when faced with disruption and stress.**

***Keywords*** *– Operational Resilience, Critical Infrastructure, Resilience Management*

## I. Extended Abstract

The United States Postal Inspection Service (USPIS) has collaborated with the CERT® Program at Carnegie Mellon University's Software Engineering Institute (SEI) to improve the security and resilience of selected United States Postal Service (USPS) products and services. Developing and implementing measurable methodologies for improving the security and resilience of a national postal critical infrastructure sub-sector directly contribute to protecting public and postal employees, assets, and revenues. Such methodologies also contribute to the security and resilience of other modes of transport and to the protection of the global supply chain.

Outcomes of this collaboration demonstrate that the use of modern resilience management frameworks and the associated techniques enable a structured, repeatable, and integrated approach for owners, operators, and regulators of critical transportation infrastructures and subsectors. This approach enables more effective planning, assessment, management, and sustainment of transportation products and services to ensure that they meet all required security, safety, and resilience needs, particularly when faced with disruption and stress.

This collaboration has included projects dealing with incident response, export screening, authentication services, physical security and aviation screening for international mail, Express Mail revenue assurance, and development of mail-specific resilience management practices for mail induction, transportation, delivery, and revenue assurance.

The CERT Resilience Management Model (CERT-RMM) and its companion diagnostic methods have served as the foundational tool for this collaboration. CERT-RMM is a capability-focused maturity model for improving an organization's management of operational resilience activities across the domains of security management, business continuity management, and aspects of information technology operations management. These improvements enable high-value services to meet their missions consistently and with high quality, particularly during times of stress and disruption.

This paper describes the USPIS/CERT collaboration, how CERT-RMM has been applied to meet USPIS project objectives, how project outcomes are contributing to improving the resilience of USPS products and services, and how similar use of CERT-RMM is applicable to other transportation critical infrastructure sectors. This includes those sectors responsible for the movement of people and goods from one physical location to another, particularly when faced with disruption and stress to transportation services.

There are strong interrelationships between postal, shipping, and transportation critical infrastructure when it comes to security, safety, and resilience. This fact is emphasized in the U. S. Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," which was issued by the President on February 12, 2013. The updated structure of the Nation's critical infrastructure sectors, which

was put in place through PPD-21, combines postal, shipping, and transportation functions into a single, overarching critical infrastructure sector. The list of subsectors in the restructured transportation sector and their key characteristics of relevance to operational resilience are summarized in Table 1 below.

| Transportation Subsectors | Primary Units of Transportation | Modes of Transportation |
|---|---|---|
| Aviation | People & Goods | Air |
| Highway Infrastructure & Motor Carrier | People & Goods | Ground |
| Maritime Transportation Systems | People & Goods | Sea |
| Mass Transit & Passenger Rail | People | Ground |
| Pipeline Systems | Oil & Gas | Ground |
| Freight Rail | Goods | Ground |
| Postal & Shipping | Mailpieces & Goods | Air, Ground, Sea |

Table 1 - U. S. Transportation Sector and Its Subsectors

The concept of operational resilience, its management, and many of the techniques imbedded in CERT-RMM, and utilized by USPS/USPIS, are directly applicable to all subsectors of the restructured transportation sector as illustrated in Table 2 below.

| Transportation Subsectors | Incident Response | Export Screening | Authentication Services | Physical Security | Revenue Assurance Risk |
|---|---|---|---|---|---|
| Aviation | X | X | X | X | X |
| Highway Infrastructure & Motor Carrier | X | | | X | X |
| Maritime Transportation Systems | X | X | X | X | X |
| Mass Transit & Passenger Rail | X | | X | X | X |
| Pipeline Systems | X | | | X | X |
| Freight Rail | X | | X | X | X |
| Postal & Shipping | X | X | X | X | X |

Table 2 - Applicability of Transportation Subsectors to USPS/USPIS Projects

Whether it is people, physical goods, oil and natural gas, or mailpieces that are being moved from one location to another, stakeholders in all transportation subsectors are concerned about very similar operational risks and are interested in the same set of core security, safety, and resilience requirements (e.g., availability, sanctity, custody, and visibility).

In addition to applications to postal and transportation critical infrastructure, principles and practices of operational resilience as captured in CERT-RMM have been successfully used to meet the resilience and cybersecurity needs of other critical infrastructure sectors. Examples include the U. S. Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model and the U. S. Department of Homeland Security's Cyber Resilience Review.