Software Engineering Institute

A Proven Method for Identifying Security Gaps in International Postal and Transportation Critical Infrastructure

Gregory Crabb, U.S. Postal Inspection Service
Julia H. Allen, Software Engineering Institute
Pamela D. Curtis, Software Engineering Institute
Nader Mehravari, Software Engineering Institute

January 2014

TECHNICAL NOTE
CMU/SEI-2013-TN-033

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by the U.S. Postal Inspection Service and ODE under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of U.S. Postal Inspection Service or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0000854

Table of Contents

List of Figures

List of Tables

Acknowledgments

The authors acknowledge the contribution to this report of Carlos D. Rodríguez, Jose R. Gonzalez, James Buthorn, and Sam Y. Lin, who served on the Universal Postal Union assessment method development and piloting teams. The authors also thank Michael Ray, U.S. Postal Inspection Service, for his review of this report. The authors would also like to acknowledge the contributions of David White (formerly with the SEI) to this body of work.

Abstract

The safety, security, and resilience of international postal, shipping, and transportation critical infrastructure are vital to the global supply chain that enables worldwide commerce and communications. But security on an international scale continues to fail in the face of new threats. Owners and operators of critical postal, shipping, and transportation operations need new methods to identify, assess, and mitigate security risks and gaps in the most effective manner possible. The U.S. Postal Inspection Service, in collaboration with the Universal Postal Union (UPU) and the CERT® Division at Carnegie Mellon University's Software Engineering Institute, developed a physical security assessment method to identify gaps in the security of international mail processing centers and similar shipping and transportation processing facilities. This assessment method and its associated field instrument are designed to be repeatable, cost effective, scalable, accurate, meaningful, and transparent. Since the method uses UPU standards as its reference, it may be used by the international community to evaluate the security of postal administrations around the world. The method also can be applied to other types of critical transportation services, such as metropolitan transit systems. This report describes the history, development approach, field experiences, and benefits of this method.

1 Introduction

In October 2010, two packages from Yemen containing explosives were discovered on U.S.-bound cargo planes of two of the largest worldwide shipping companies, UPS and FedEx [CNN 2010, Perez 2010]. The visibility of this incident brought regulatory attention to a long-standing problem. *The Wall Street Journal* reported, "International cargo shipments have for years been seen as a weak link in anti-terror efforts. Lawmakers have stressed the importance of bolstering cargo screening for explosives, but much emphasis has focused on material loaded into passenger rather than cargo planes" [Perez 2010]. In early 2012, the Universal Postal Union (UPU) and several stakeholder organizations developed two security standards to improve security in the transport of international mail and to improve the security of critical postal facilities.

Developers of the standards recognized a need for some means to enable implementation of the new standards and measure compliance to them. The U.S. Postal Inspection Service (USPIS), the UPU, and the CERT® Division at Carnegie Mellon University's Software Engineering Institute (SEI) collaborated to develop a physical security assessment method and an associated field instrument based on the UPU standards.[1] The method can be used to identify gaps in the security of international mail processing centers and similar shipping and transportation processing facilities. In this report, we present the development approach, field experiences, benefits, and potential applications of the method for other types of critical transportation services.

[1] CERT® is a registered mark of Carnegie Mellon University.

2 Background

The UPU, headquartered in Berne, Switzerland, is a unit of the United Nations that regulates the postal services of 192 member countries. These postal services form the largest physical distribution network in the world. The Foreword to the *Postal Security Standards* states, "More than 5 million postal employees working in over 660,000 post offices all over the world handle an annual total of 434 billion letter-post items in the domestic service and 5.5 billion in the international service. More than 6 billion parcels are sent by post annually" [UPU 2013a].

The Postal Security Group (PSG) of the UPU develops global and regional security strategies to assist postal operators in their common security missions. As the UPU describes its role, "Through training initiatives, consulting missions, and prevention programs, the PSG strives to protect the employees and assets of the postal operators along with safeguarding the mails from fraud, theft and misuse" [UPU 2013a]. PSG members are security experts from a number of UPU member countries.

The PSG, together with other UPU stakeholders, developed two security standards in 2012 in response to the attempted shipment of explosives from Yemen [UPU 2011] and other similar incidents:

- *S58, Postal Security Standards – General Security Measures* defines the minimum physical and process security requirements applicable to critical facilities within the postal network [UPU 2013a].
- *S59, Postal Security Standards – Office of Exchange and International Airmail Security* defines minimum requirements for securing operations relating to the transport of international mail [UPU 2013b].

The UPU standards define mandatory measures to better screen and take custody of international mail and to apply security requirements in critical facilities, such as international offices of mail exchanges, which process arriving and departing international mail [UPU 2012]. The standards were accepted at the 25th Universal Postal Congress in Doha, Qatar, in September 2012 [UPU 2013c].

2.1 USPIS Involvement

For the past 17 years, the chief postal inspector of the USPIS has chaired the PSG, and USPIS inspectors participated in the development of S58 and S59. The USPIS is the law enforcement arm of the U.S. Postal Service (USPS). It is the longest standing federal law enforcement agency in the United States, dating back to 1772. The United States is the only country to have a separate and distinct postal inspection service. The USPIS website describes its mission and responsibilities:

> *The mission of the U.S. Postal Inspection Service is to support and protect the U.S. Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail. Through its security and enforcement functions, the Postal Inspection Service provides assurance to American businesses for the safe exchange of funds and securities through the*

U.S. Mail; to postal customers of the "sanctity of the seal" in transmitting correspondence and messages; and to postal employees of a safe work environment. [USPIS 2013]

As a member of the PSG, USPIS Inspector in Charge Gregory Crabb saw the need for a simple, lightweight assessment method for determining the capabilities of postal organizations against the new standards. In a presentation to the UPU in February 2012, Crabb proposed several objectives that could be achieved through this effort [Gregory Crabb, unpublished data]:

- improve security practices (as participating organizations made whatever adjustments the assessments revealed as necessary to meet the standards)
- demonstrate assessed organizations' capabilities to regulators (the European Commission, the International Air Transport Association, the International Civil Aviation Organization, the World Customs Organization, and internal and external governance bodies)
- assess security suppliers
- have the PSG serve as the independent validator for the European Commission

2.2 Collaboration with the CERT Division

Since 2011, the USPIS has collaborated with the SEI's CERT Division to improve the resilience of selected USPS products and services. 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 Division is the largest technical program at the SEI, a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University. CERT staff conduct research and development in internet security, secure systems, operational resilience, and coordinated response to security incidents.

Much of the USPIS work with the CERT Division related to the CERT Resilience Management Model (CERT-RMM), 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. Crabb asked the CERT Division to develop an assessment method for the UPU standards based on the CERT-RMM assessment method and process, along with a companion field instrument with automated features.

These were the design criteria for the method and the instrument:

- repeatable: The method can be used consistently by different independent teams in the same situation to acquire the same results.
- cost effective and scalable: The method is economical and functional for all locations, regardless of size or capability.
- accurate: The method is evidence-based and derived from international standards so that results can be relied on by the international community (e.g., UPU, International Civil Aviation Organization, International Air Transport Association, Transportation Security Administration, and World Customs Organization).

- meaningful: The method generates results that can easily be acted on by owners and operators of the assessed processing facilities.
- transparent: The method is publicly available and can be used for self-assessment.

The method was designed to allow assessed postal organizations to gain insight into their capabilities by identifying the strengths and weaknesses of their current security practices. Assessment results could also identify risks and inform the prioritization of security improvements.

3 Method Development and Description

USPIS and CERT staff held several work sessions in January and February 2012 to develop the first version of the method and instrument for piloting in February. The S58 and S59 postal security standards served as the requirements for the method and were annotated to facilitate the formulation of assessment questions. The team continued to develop and improve the method based on pilot assessments in three locations worldwide. The method and field instrument were released for public use in September 2012, and a number of additional locations have applied them since then. Updates to the method require UPU approval.

As depicted in Figure 1, the method defines three phases for conducting the assessment:

- Preparation: Analyze requirements, develop an assessment plan, select and prepare the assessment team, send and receive the pre-assessment questionnaire, obtain and inventory objective evidence, and prepare for the conduct of the assessment (initial site visit and logistics).
- On-site: Prepare participants, conduct interviews, examine objective evidence, document objective evidence, verify objective evidence, perform characterizations and ratings, formulate and validate preliminary findings, generate the final results of the assessment, and identify improvements to the method and the standards.
- Reporting: Deliver assessment results to sponsors and key stakeholders, and preserve and archive assessment results.

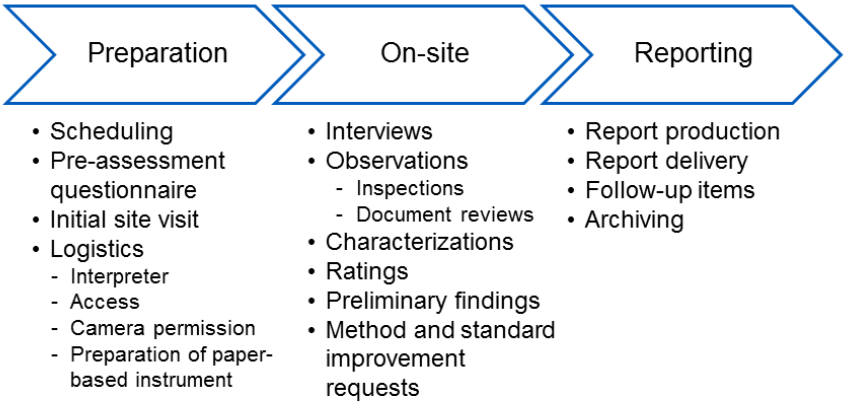

Figure 1: Phases of the Method

The assessment method contains a series of questions based on the requirements in the S58 and S59 standards (refer to Table 1 for examples) [UPU 2013c]. The method also defines the evidence requirements for each section of the standards. The team conducting the assessment must see documented artifacts or receive oral and written statements and affirmations confirming or supporting implementation (or lack of implementation) of a practice. If there are specific weaknesses in implementation, team members record them on their assessment worksheets. For example, a weak-

ness in implementation of S58 Section 5.1.1, Risk Assessment and Facility Security Plans, might be that the facility's security plan covers general lighting requirements but not interior emergency lighting.

Table 1: S58 Requirements and Assessment Questions

S58 Section	S58 Requirement	Assessment Question
5.1.1	"An annual risk assessment must be conducted to identify each critical facility. The assessment shall take into consideration the postal assets and operations at the facility, the general crime rate of the areas and other contributing factors that increase the likelihood of criminal incidents" [UPU 2013a].	Do you conduct an annual risk assessment for each critical facility? If so, would you please provide two recent risk assessment reports for review? Does the risk assessment report consider the postal assets and operations at the facility, the general crime rate of the area, and other contributing factors that increase the likelihood of criminal incidents?
5.2.2	"A visitor registration system shall be implemented to record entries of non-employees into secure areas of the critical facility" [UPU 2013a].	Are visitors provided with identification badges so they can be positively identified when entering secure areas?
6.2	"A termination process must be documented for employees and contractors. The termination process ensur[es] the timely return of identification documents, access control devices, keys, uniforms and other sensitive information. A record system must be maintained to prevent rehiring of terminated employees or contractors" [UPU 2013a].	Do you have a documented termination process? If yes, please share the documentation. Does the termination process ensure the timely return of identification documents, access-control devices, keys, uniforms, and other sensitive information? Do you have a record system to prevent rehiring employees or contractors who have been terminated for cause?
7	"After screening or the application of other security controls, mail shall be accounted for and protected from unauthorized interference prior to loading on an aircraft or secure exchange with the carrier, ground handling agent or other contractor" [UPU 2013a].	After security controls have been applied, how is mail accounted for and protected from unauthorized interference prior to loading on an aircraft or secure exchange with the carrier, ground handling agent, or other contractor?

The assessment team considers the results of interviews and the other evidence collected to reach a consensus on subsection characterizations and section ratings.

Subsections are characterized using the FILIPINI scale and rules (see Figure 2):

- Fully Implemented (FI): One or more direct artifacts are present and judged to be acceptable; at least one indirect artifact or affirmation exists to confirm the implementation; and no weaknesses are noted.
- Largely Implemented (LI): One or more direct artifacts are present and judged to be adequate; at least one indirect artifact or affirmation exists to confirm the implementation; and one or more weaknesses are noted.
- Partially Implemented (PI): Direct artifacts are absent or judged to be inadequate; one or more indirect artifacts or affirmations suggest that some aspects of the practice are implemented; and one or more weaknesses are noted. Alternatively, one or more direct artifacts are present and judged to be adequate; no other evidence (indirect artifacts, affirmations) supports the direct artifact(s); and one or more weaknesses are noted.
- Not Implemented (NI): Direct artifacts are absent or judged to be inadequate; no other evidence (indirect artifacts, affirmations) supports the practice implementation; and one or more weaknesses are noted.

- Not Applicable (NA): The standard section does not apply (e.g., in the S58 standard, Section 6.2, "Contractor Security Requirements," applies only to organizations that use contractors for mail handling/transport operations or other sensitive functions).

Sections are rated more simply, since the goal of the assessment is essentially to arrive at a "Yes" or "No" judgment for each set of practices that constitute a section:

- Satisfied: All associated practices are characterized as FI, LI, or Not Applicable, with at least one practice characterized as FI or LI; and the aggregation of weaknesses does not have a significant negative impact on goal achievement.
- Not Applicable: All practices are characterized as Not Applicable.
- Not Satisfied: All other cases (i.e., the rules for Satisfied [S] and Not Applicable [NA] are not met).

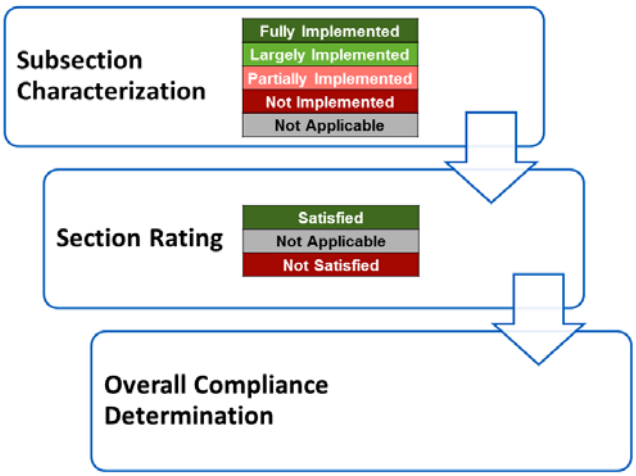

Figure 2: Steps in Compliance Determination

The assessment team repeats the on-site process for all subsections of the standard, as shown in Figure 3, beginning with "Conduct Interviews." The assessment team then creates a heat map of the results, as shown in Figure 4. To satisfy the standard, all section-level ratings for the facility must be Satisfied or Not Applicable.

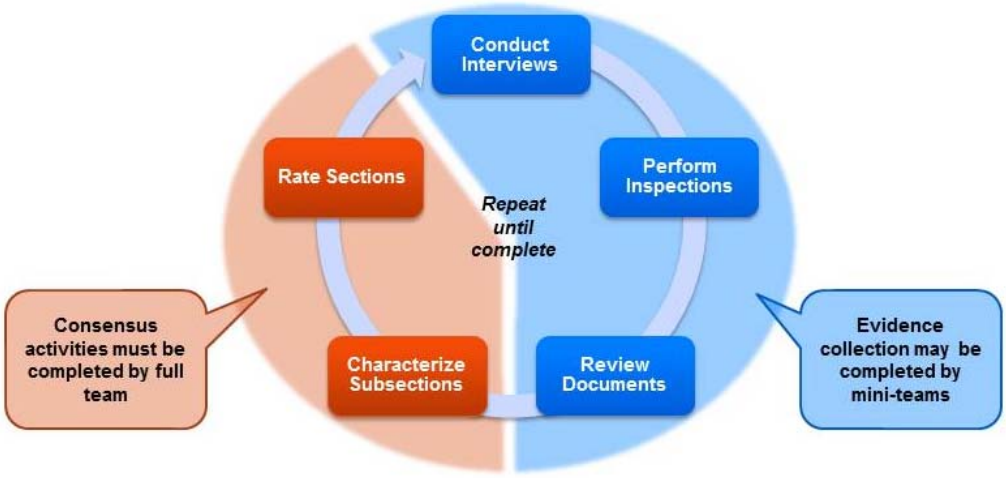

Figure 3: On-site Process of Collecting Evidence and Reaching Consensus on Characterizations and Ratings

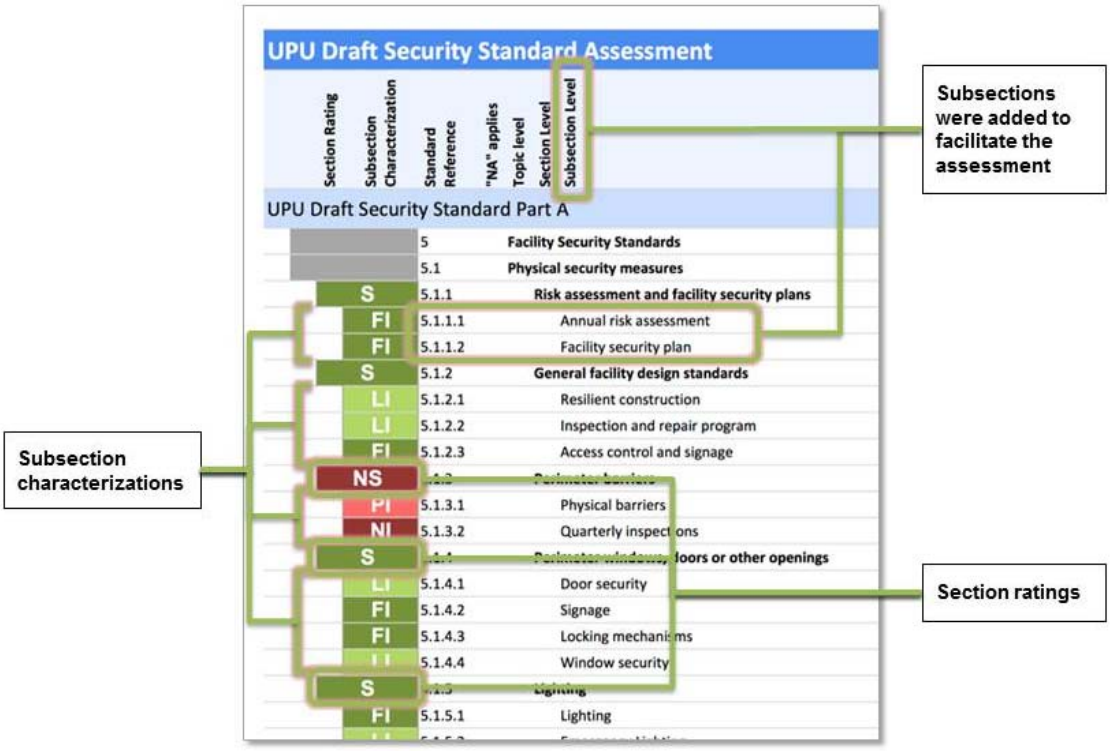

Figure 4: Sample Heat Map of Assessment Results

Note: FI = Fully Implemented; LI = Largely Implemented; PI = Partially Implemented; NI = Not Implemented; S = Satisfied; NS = Not Satisfied.

4 Field Experiences

In February 2012, USPIS staff conducted the first pilot assessments using the new method with draft versions of S58 and S59. The USPIS continued to conduct assessments and work with CERT staff to improve the method throughout 2012. CERT staff also recommended some improvements to the content of the standards to the UPU.

As a result of one assessment, the country postmaster general closed down the facility where international mail was being dispatched and moved operations to a new facility with improved security controls and conformance with UPU standards. Other reviews have shown that postal administrations largely conform to UPU standards and that having the specific feedback of assessment results encourages them to make the minor improvements needed to ensure full compliance.

One consistent finding highlighted the effectiveness of the method for producing accurate assessments. The S58 standard requires a single, written security plan for critical facilities. Each pilot location had a security plan, but it did not contain all the elements that the standard requires. But in following the method's evidence-discovery procedures, the assessment team found the missing elements in other documents, such as maintenance plans.

The S58 standard requires that access control systems be used for employees, visitors, service providers, and vendors of critical facilities but does not specify any particular system. At all locations examined in the pilots, the assessment team found some failing in this requirement. But many postal organizations operate at a deficit, so the team tailored its compliance recommendations to each organization's fiscal realities.

None of the pilot locations had plans for crisis planning and business continuity. However, employees generally knew what to do in crisis situations, so the postal administrations had only to document that knowledge to reach compliance.

All of the pilot locations have asked to be reassessed after making the improvements recommended in their initial assessments.

4.1 Benefits

Based on field reports and assessment results, participating postal organizations have realized the following benefits:

- gained insight into their capability by identifying the strengths and weaknesses of current security practices
- achieved recognition as having a strong security posture by the International Civil Aviation Organization, World Customs Organization, and supply chain partners that rely on postal services for moving goods
- obtained guidance to prioritize security-related improvement plans
- received feedback on the maturity level of the organization's security program
- were able to better identify and prioritize security risks

5 Conclusion

Pilot organizations have shown that using a structured, scripted assessment instrument is an effective way to assess compliance with the UPU postal security standards. The USPIS and other postal sector organizations continue to use the assessment method today to achieve initial results and assess progress made after implementing improvements. In 2014, the method will be provided to civil aviation authorities, who will use it primarily to assess the performance of postal administrations in meeting the screening and other international airmail security standards of S59.

The method can be tailored and applied to other types of critical transportation services, including those that move people (such as metropolitan area transit systems) and goods by air, ground, and sea, and to other safety and security standards. It can thus serve as a practical and lightweight way to implement and measure compliance to standards for ensuring the safety, security, and resiliency of international postal, shipping, and transportation infrastructure.

References

URLs are valid as of the publication date of this document.

[CNN 2010]
CNN Wire Staff. "Yemen-Based al Qaeda Group Claims Responsibility for Parcel Bomb Plot." *CNN International Edition*, November 6, 2010. http://edition.cnn.com/2010/WORLD/meast/11/05/yemen.security.concern/?hpt=T2http://www.npr.org/templates/story/story.php?storyId=130935022

[Perez 2010]
Perez, E.; Entous, A.; & Coker, M. "Yemeni Bombs Target U.S." *Wall Street Journal*, October 29, 2010. http://online.wsj.com/article/SB10001424052702303284604575582273576079534.html?KEYWORDS=Yemen+Air+Cargo+Incident

[UPU 2011]
Universal Postal Union. "UPU to Develop Global Postal Security Standards." *25th Universal Postal Congress*, April 18, 2011. http://dohacongress.upu.int/home/singel-news/article/upu-to-develop-global-postal-security-standards

[UPU 2012]
Universal Postal Union. "Progress Made on New Postal Security Standards." *UPU News*, March 8, 2012. http://news.upu.int/nd/progress-made-on-new-postal-security-standards

[UPU 2013a]
Universal Postal Union. *Postal Security Standards: General Security Measures* (S58). UPU, July 2013. http://www.upu.int/uploads/tx_sbdownloader/standardS58PostalSecurityEn.pdf

[UPU 2013b]
Universal Postal Union. *Postal Security Standards: Office of Exchange and International Airmail Security* (S59-1). UPU, July 2013. http://www.upu.int/uploads/tx_sbdownloader/standardS58PostalSecurityEn.pdf

[UPU 2013c]
Universal Postal Union. *Postal Security Standards*. UPU, 2013. http://www.upu.int/en/activities/postal-security/security-standards.html

[USPIS 2013]
U.S. Postal Inspection Service. *Mission*. USPIS, 2013. https://postalinspectors.uspis.gov/aboutus/mission.aspx

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
A Proven Method for Identifying Security Gaps in International Postal and Transportation Critical Infrastructure	FA8721-05-C-0003

6. AUTHOR(S)

Gregory Crabb, Julia H. Allen, Pamela D. Curtis, and Nader Mehravari

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-TN-033

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

The safety, security, and resilience of international postal, shipping, and transportation critical infrastructure are vital to the global supply chain that enables worldwide commerce and communications. But security on an international scale continues to fail in the face of new threats. Owners and operators of critical postal, shipping, and transportation operations need new methods to identify, assess, and mitigate security risks and gaps in the most effective manner possible. The U.S. Postal Inspection Service, in collaboration with the Universal Postal Union (UPU) and the CERT® Division at Carnegie Mellon University's Software Engineering Institute, developed a physical security assessment method to identify gaps in the security of international mail processing centers and similar shipping and transportation processing facilities. This assessment method and its associated field instrument are designed to be repeatable, cost effective, scalable, accurate, meaningful, and transparent. Since the method uses UPU standards as its reference, it may be used by the international community to evaluate the security of postal administrations around the world. The method also can be applied to other types of critical transportation services, such as metropolitan transit systems. This report describes the history, development approach, field experiences, and benefits of this method.

14. SUBJECT TERMS	15. NUMBER OF PAGES
international shipping security, international transportation security, international mail security, risk assessment, risk mitigation, UPU standards, CERT-RMM, resilience management	25

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL