



Department of Homeland Security Office of Inspector General

Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure

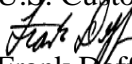




Homeland Security

September 28, 2011

MEMORANDUM FOR: Charles Armstrong
Assistant Commissioner
Office of Information and Technology
U.S. Customs and Border Protection

FROM: 
Frank Deffer
Assistant Inspector General
Information Technology Audits

SUBJECT: *Final Letter Report: Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure*

Attached for your information is our final letter report, *Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure*. We incorporated the formal comments from U.S. Customs and Border Protection in the report.

The report contains three recommendations aimed at improving U.S. Customs and Border Protection's overall effectiveness in securing its wireless infrastructure. Your office concurred with all of the recommendations. Within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. The report will be posted on our website.

Should you have any questions, please call me, or your staff may contact Richard Saunders, Director, Advanced Technology Division, at (202) 254-5440.

Attachment

Appendix B

Managements Comments to the Draft Letter Report

3

Recommendation #3: Establish a process to perform regular vulnerability assessments to evaluate the effectiveness of the Enterprise Wireless Infrastructure's wireless security and to detect unauthorized wireless networks and devices.

CBP Response: Concur. Vulnerability scans have been set up for all EWI Wireless Controllers. Vulnerability Assessment Team (VAT) scans are currently being conducted by the Wireless Information Systems Security Officer (ISSO). A schedule will be formalized by December 2011 to ensure the scans are conducted on a regular and recurring basis.

Completion Date: December 31, 2011

With regard to the sensitivity of the draft report, CBP did not identify any sensitive information that would require a "For Official Use Only" designation or warrant protection under the Freedom of Information Act.

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Ashley Boone, CBP Audit Liaison, at (202) 344-2539.

Appendix C
Major Contributors to this Report

Richard Saunders, Director
Steve Matthews, IT Audit Manager
Philip Greene, IT Audit Team Leader
Jamie Horvath, IT Specialist
Patrick Nadon, Report Consultant
Frederick Shappee, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Information Officer
Chief Information Security Officer

Customs and Border Protection

CBP Commissioner
CBP Chief Information Officer
CBP Chief Information Security Officer
CBP Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committee, as appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.