U.S. Customs and Border Protection

Attachment C

Information Systems Security Officer (ISSO) Designation Letter

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release based solely on DHS 4300A, Version 6.1.1, attachment. There are no substantive differences between this CBP attachment and its source DHS attachment. This attachment is included as part of the CBP 1400-05D handbook suite to enable the CBP user to be able to access all IT security policies (DHS as well as CBP specific) at one location.
2.0	December 21, 2010	No changes.

DHS Information Systems Security Officer (ISSO) / Alternate Information Systems Security Officer (AISSO) Designation

The following person is designated as the ☐ ISSO / ☐ AISSO for the _____ (major application or general support system, as appropriate)

Name	
DHS Component	
Title	
Office	
Telephone Number	
E-mail Address	

Affiliation (select one)

☐ CBP Employee.

☐ CBP Support Contractor. If support contractor, provide name of contracting company: _____

Designating Official (System Owner, Senior Site Manager, or ISSO, as appropriate)

Name: _____ Title: _____

Signature: _____ Date: _____

Review and Approval (by the Chief Information Security Officer)

Name: _____ Title: _____

Signature: _____ Date: _____

Comments: _____

ISSO / AISSO Acknowledgment of Responsibilities

I, _____ (print name), have been formally designated an ☐ Information Systems Security Officer (ISSO) / ☐ Alternate Information Systems Security Officer (AISSO) for the _____ (major application or general support system, as appropriate), and I understand that I am responsible for coordinating information technology security regulations and requirements as described in appropriate security policy publications and handbooks including the following:

- Ensuring that security requirements for the major application or general support system with which I am involved are being or will be met.
- Ensuring that requests for certification and accreditation of computer systems are completed in accordance with the published procedures.
- Ensuring that protective measures for physical security threats such as deadbolt locks on doors, placement of electrical wiring, etc., are in place.
- Ensuring compliance with all legal requirements concerning the use of commercial proprietary software, e.g., respecting copyrights and obtaining site licenses.
- Maintaining an inventory of hardware and software within the program/development offices or field site facility.
- Coordinating the development of a Contingency Plan and ensuring that the plan is tested and maintained.
- Ensuring risk analyses are completed to determine cost-effective and essential safeguards.
- Ensuring preparation of security plans for sensitive systems and networks.
- Attending security awareness and related training programs and distributing security awareness information to the user community as appropriate.
- Reporting IT security incidents (including computer viruses) in accordance with established procedures.
- Reporting security incidents not involving IT resources to the appropriate security office.
- Providing input to appropriate IT security personnel for preparation of reports to higher authority concerning sensitive and/or national security information systems.

DHS Component: _____

Office: _____ Telephone Number: _____

Signature _____ Date _____