

***U.S. DEPARTMENT OF COMMERCE  
Office of Inspector General***

---



***Bureau of Industry and Security***

***FY 2009 FISMA Assessment of  
Bureau Export Control Cyber  
Infrastructure, Version 2  
(BECCI-2)***

*Draft Inspection Report No. OSE-19575/September 2009*

*Office of Audit and Evaluation*





**UNITED STATES DEPARTMENT OF COMMERCE**  
**Office of Inspector General**  
Washington, D.C. 20230

September 30, 2009

**MEMORANDUM FOR:** Daniel O. Hill  
Acting Under Secretary for Industry and Security and  
Deputy Under Secretary for Industry and Security

A handwritten signature in cursive script, reading "Allen Crawley", is positioned above the typed name.

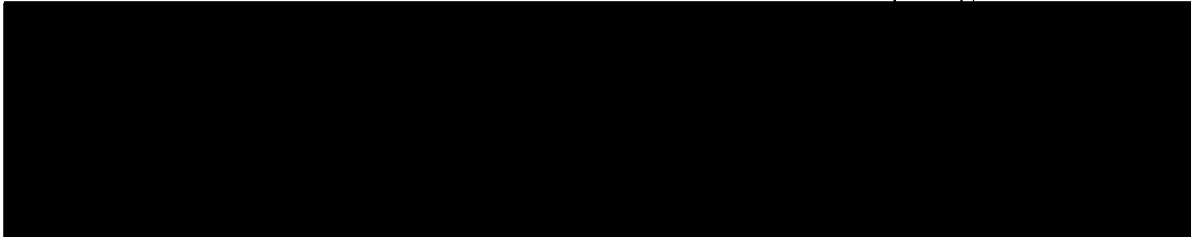
**FROM:** Allen Crawley  
Assistant Inspector General  
for Systems Acquisition and IT Security

**SUBJECT:** Bureau of Industry and Security  
*FY 2009 FISMA Bureau Export Control Cyber  
Infrastructure, Version 2 (BECCI-2)*  
Final Inspection Report No. OSE-19575

This report presents the results of our Federal Information Security Management Act (FISMA) review of BIS' certification and accreditation of the Bureau Export Control Cyber Infrastructure, Version 2 (BECCI-2).

We found that BIS' certification and accreditation of BECCI-2 did not meet Department and FISMA requirements. We identified deficiencies with security planning, a lack of defined configuration settings prior to the security certification, and an incomplete security control assessment. In addition, the authorizing official's accreditation decision did not comply with Department and BIS policy, and as a result, additional oversight of the system may have been inappropriately avoided. We also found that reporting procedures required by Department policy were not followed.

OIG's own assessment of BECCI-2 controls found vulnerabilities requiring remediation.



In its response to our draft report, BIS did not dispute our findings but did not specifically indicate whether it agreed with our recommendations. After receiving BIS's response, I spoke with BIS' acting chief information officer, who stated that BIS agreed with our findings and recommendations. BIS' response is included in its entirety as appendix C.

We request that you provide us with an action plan describing the actions you have taken or plan to take in response to our recommendations within 60 calendar days of the date of this report. A plan of action and milestones should be used to communicate the plan as required by FISMA.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you would like to discuss any of the issues raised in this report, please call me at (202) 482-1855.

Attachment

cc: Suzanne Hilding, chief information officer, U.S. Department of Commerce  
Eddie Donnell, acting chief information officer, BIS  
Raushi Conrad, director, System and Security Operations, BIS

## Listing of Abbreviated Terms and Acronyms

AAA	Authentication, Authorization, and Accounting (██████ feature)
ACL	Access Control List
ATO	Authorization to Operate
BECCI-2	Bureau Export Control Cyber Infrastructure, Version 2
BIS	Bureau of Industry and Security
C&A	Certification and Accreditation
CIO	Chief Information Officer
CIS	Center for Internet Security
CSAM	Cyber Security Assessment and Management
DISA	Defense Information Systems Agency
DoD	Department of Defense
ECASS-R	Export Control Automated Support System Redesign
██████	████████████████████
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IATO	Interim Authorization to Operate
IMS-R	Investigative Management System - Redesign
IT	Information Technology
ITSO	Information Technology Security Officer
██████	████████████████████
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OITPP	Office of IT Policy and Planning
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
██████	████████████████████
SOP	Standard Operating Procedures
SSP	System Security Plan
UPI	Unique Project Identifier
██████	████████████████████

## Synopsis of Findings

- Key security planning activities necessary for certification and accreditation were not performed.
- Secure configuration settings were not defined for information technology (IT) products prior to the security control assessment.
- Security control assessment was not adequate for a [REDACTED] system.
- Authorizing official's accreditation decision violated Department and Bureau of Industry and Security (BIS) IT security policy and Federal Information Security Management Act of 2002 (FISMA) guidance.
- Reporting procedures required by Department IT policies were not followed.
- OIG control assessment found vulnerabilities requiring remediation.

## Conclusion

The certification and accreditation of the Bureau Export Control Cyber Infrastructure, Version 2 (BECCI-2) did not meet Department and FISMA requirements for a [REDACTED] system. Security planning deficiencies, in particular, the lack of defined security requirements, undermined the certification team's ability to assess controls accurately and completely. Without defined security requirements, the certification team was left to judge controls against best practice standards rather than those that are customized to the needs of the system. This was most evident with the Configuration Settings (CM-6) control where no secure settings had been defined and documented for IT products, although BIS has since made progress in this area.

In many cases, necessary testing was not performed and control assessments consisted of interviews and examination of incomplete documentation. Many IT products were not assessed because their existence was unknown to the certification team in time to adequately prepare assessment procedures.

The certification team asserted its penetration test demonstrated the capability of BECCI-2 defenses. However, we remain concerned with BIS' [REDACTED]  
[REDACTED]

While budget constraints led BIS to focus its resources in some areas at the expense of others, FISMA requires the depth and rigor of security planning and the intensity of security control assessments be scaled to BECCI-2's [REDACTED]  
[REDACTED]  
[REDACTED]

### **Summary of BIS Response**

In its response to our draft report, BIS did not dispute our findings but did not specifically indicate whether it agreed with our recommendations. BIS stated that in FY 2010 it plans to have a complete and approved certification and accreditation for all its systems. BIS also stated it has begun efforts to improve certification and accreditation documentation, IT workforce skills, and overall FISMA responsibilities.

BIS' response is included in its entirety as appendix C of this report.

### **OIG Comments**

After receiving BIS' response, OIG's assistant inspector general for systems acquisition and IT security spoke with BIS' acting chief information officer, who stated that BIS agreed with our findings and recommendations.

## Introduction

BECCI-2 is the production version general support system that was implemented as part of BIS' Export Control Automated Support System Redesign (ECASS-R). BECCI-2 is part of an effort that began in 2006 to implement an infrastructure designed to segregate applications according to the categorization of information stored, processed, and transmitted.

The system is intended to host BIS' major applications that include [REDACTED]

The system consists of network components, security infrastructure, storage and system administration software and hardware components, servers, and workstations. The system includes data centers in [REDACTED], and additional components in the [REDACTED]. Redundant connections to the data centers exist via the [REDACTED]. There are also field offices located throughout the United States that include network components and workstations for major application users.

Thus far, and for the duration of our evaluation, only one major application is operating on the BECCI-2 infrastructure; this application, the Investigative Management System-Redesign (IMS-R), is separately certified and accredited and not part of our review.

## Certification and Accreditation (C&A) Timeline and BIS' Constraints

BECCI-2's security certification occurred during August-September 2008, and the system was authorized to operate on October 3, 2008. In a memo submitted with the C&A package, BIS told us that

Given the severe BIS 2008 and 2009 budget constraints, BIS made a conscious decision, with the cognizance of the Under Secretary, Deputy Under Secretary, Department CIO, Department Deputy Secretary, and the full Department IT Review Board, to focus its very scarce resources on technical controls as opposed to documentation.

The memo also indicated that BIS' executive management considered delaying BECCI-2's deployment until securing "additional funding to improve its documentation and address all" of the certification team's findings. However, a previous [REDACTED] on the [REDACTED] made the deployment of IMS-R onto BECCI-2 infrastructure "critical." And BIS indicated, "Consideration of the design, [sic] is a driver (in addition to its technical controls testing results) for the independent...assessment of the system as secure."

The authorizing official's accreditation decision letter, while granting a "full" authorization to operate (ATO), placed restrictions on system operation by requiring the system owner and staff to mitigate high- and moderate-risk vulnerabilities within 180 days, or the authorization to operate would be rescinded. On April 1, 2009, the system owner requested, and the authorizing official granted, a 6-month extension of the ATO in order to complete the mitigation of vulnerabilities.

## Findings and Recommendations

### 1. Key Security Planning Activities Necessary for Certification and Accreditation Were Not Performed

*Background: Department policy requires operating units to follow the C&A process as detailed in NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. NIST SP 800-37 outlines a four-phased<sup>1</sup> process to ensure “agency officials have the most complete, accurate, and trustworthy information possible on the security status of information systems.” The initiation phase includes security planning activities, which provide a basis for the assessment of security controls in the security certification phase.*

- The system’s accreditation boundary was not defined prior to the security certification phase.
  - The certification team was not provided a complete listing of the system’s hardware and software components, required by Department policy, which would fully describe the system’s accreditation boundary.
    - This lack of information hampered the security control assessment (see finding 3).
  - The initiation phase in NIST SP 800-37 calls for the system owner to confirm that the system has been fully described and documented before beginning the security certification phase.
- The system security plan was incomplete and did not provide an adequate basis for the security certification.
  - Draft versions<sup>2</sup> of the security plan given to the certification team were missing sufficient detail to permit analysis and testing of controls.
    - [REDACTED] This level of assurance was not evident in the security plan and related system documentation.
      - [REDACTED] technical controls descriptions we examined were inadequate in the security plans BIS provided to the certification team for its control assessment. (This includes information in the “Detailed Network and Security Infrastructure Design” document that the certification team referenced in its assessment results.)

<sup>1</sup> The four phases of the C&A process are: initiation, security certification, security accreditation, and continuous monitoring.

<sup>2</sup> The certification team’s spreadsheet of assessment results references security plan versions 0.2, 0.3, and 0.4. We reviewed draft Versions 0.3 and 0.4 and BIS-approved Versions 1.0 and 1.5.

<sup>3</sup> From NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, E-1-2



- The certification team told us that the lack of information in the plan precluded testing many controls. In its security assessment report, the certification team said, "The [system security plan] is still in draft form during conduct of the [security control assessment] and test development. It contains references to documents that are unknown to the testers, or currently do not exist."
  - The security assessment report also noted, "The primary reason for most [control] failures was material weakness of policy, procedures, plans, and records," indicating, "This is an administrative corrective action that **impacts technical controls** [emphasis added]."
- The approved system security plan (Version 1.0) was not completed until after most of the security control assessment and was not provided to the certification team.
  - The security plan was approved by the system owner, BIS' then-chief information officer (CIO), and the information technology security officer (ITSO) on August 29, 2008, and by the authorizing official on September 5, 2008.
  - The certification team assessed controls between August 18, 2008, and September 15, 2008, and told us BIS did not provide the approved security plan.
    - Even if it had, we found Version 1.0 to have the same deficiencies as the draft plans. BIS has improved its security plan since the accreditation with Version 1.5, which provides more complete information on control implementations.
  - NIST SP 800-37 calls the acceptance of the security plan by the authorizing official and senior agency information security officer "an important milestone" that occurs "prior to conducting an assessment of controls."
- Common security controls<sup>4</sup> were not clearly defined.
  - The initial security plan identified 35 security controls as common controls (controls the system inherits from others), or having partially common control elements, because they were controls supporting several IT systems including BECCI-2.
  - The certification team noted, in the security assessment report, some uncertainty about "inheritance from the enterprise" and whether the system owner has responsibility for some controls.
  - After certification and accreditation was completed, BIS asserted that BECCI-2 does not have common controls that it inherits from other providers, but it is providing controls for all other systems residing on its infrastructure.
    - This change illustrates the fact that several months after certification testing was completed, there was still uncertainty as to who was responsible for security controls in BECCI-2.

<sup>4</sup> Common security controls' development, implementation, and assessment are assigned to responsible organization officials or elements other than system owners whose systems will implement or use the controls. Common controls are intended to facilitate reuse across systems where they will be used (see NIST SP 800-53, Rev. 2, 9-10).

## **Recommendations**

BIS should

- 1.1 provide a full listing of hardware and software components in advance of future control assessments so that assessors may prepare for testing of all IT products where controls are implemented;
- 1.2 include in the system security plan and related documents sufficient detail to permit analysis and testing of controls;
- 1.3 ensure that updated security plans are accepted by the system owner, authorizing official, and BIS' ITSO in advance of future control assessments; and
- 1.4 in the event that common controls are employed, update the plan to provide sufficient clarity as to who is responsible for their development, implementation, and assessment.

## 2. Secure Configuration Settings Were Not Defined for IT Products Prior to the Security Control Assessment

*Background: The Department's IT security policy and NIST SP 800-53 require establishing and assessing secure configuration settings for IT products, which include operating systems for system components (such as servers, desktops, laptops, routers, and switches) and applications (such as e-mail, Web, virtual private network (VPN), firewall, intrusion detection, database, and antivirus). FISMA and OMB guidance also highlight the importance of secure configuration settings. Implementing and maintaining secure configuration settings is one of the most effective ways of negating threats.*

- Secure configuration settings were not defined prior to the assessment of controls by the certification team.
  - The certification team indicated the Configuration Settings (CM-6) control was not tested on system components "due to time constraints" and said, "This test should be completed during the next assessment."
  - The certification team did compare configuration settings of some IT products against Defense Information Systems Agency (DISA)-defined settings or industry best practices.
    - Settings from [REDACTED] were examined in this manner.
    - While the scanning revealed deficiencies, the certification team could not validate settings based on the specific operational needs of this [REDACTED] system because BIS had not defined its own settings. Therefore, the risk presented by the deficiencies was not clear.
- Currently defined configuration settings for IT products need improvement.

BIS has now defined configuration settings for IT products on BECCI-2. Below, we present deficiencies that should be addressed. (The NIST SP 800-53 assurance requirements for a [REDACTED] system like BECCI-2 call for [REDACTED].)

Department IT security policy requires operating units to implement the methodology described in NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*. NIST SP 800-70 calls for organizations to tailor industry standards or checklists (benchmarks) to reflect local rules, regulations, and mandates. Any changes to the standard checklist or other industry guide should be documented as part of the organization's defined configuration settings. BIS has not documented some of its configuration settings according to these requirements.

- The file defining BIS' [REDACTED] standard secure configuration does not explain deviations from benchmark settings.
  - BIS used "[REDACTED] Security Guide and the [Center for Internet Security (CIS)] [REDACTED] ... Consensus Security Settings ... as the basis for configuring the systems and customized the settings ..."
  - A review of the file defining BIS' custom settings found that the rationale for modifications to benchmark settings was not explained.

- OIG identified [REDACTED] vulnerabilities through DISA-based testing (Gold Disk). BIS indicated that these were not vulnerabilities stating, "It is a compliance issue as relates to Gold Disk standards. We do not set our [configuration settings] to adhere to Gold Disk standards. (And there is nothing in the [system security plan] that contradicts the settings used on these servers.)"
  - However, while BIS may not adhere to Gold Disk standards in its standard secure configuration, the Gold Disk vulnerabilities, according to DISA, have a high potential of giving access to an intruder.
  - In addition, there is overlap between DISA's Gold Disk and BIS' defined settings since many of DISA's recommended settings are derived from settings recommended in the benchmarks used by BIS.
    - Of the seven vulnerabilities from our DISA-based testing that we discussed with BIS, four are addressed in the [REDACTED] Security Guide, which BIS cites as a benchmark (see table 5 for details).
- BIS' secure configuration settings for [REDACTED] devices need improvement.
  - BIS' standard secure configuration for [REDACTED] devices is based on CIS and NSA benchmarks. The BIS standard secure configuration depicts the BECCI-2 configuration settings in relation to CIS' recommendations.
  - Not all benchmark settings are addressed in BIS' [REDACTED] standard secure configuration. Notably:
    - Authentication, authorization, and accounting (AAA) security mechanisms – The BIS standard secure configuration addresses only authentication. The benchmarks include recommendations for configuring authorization and accounting mechanisms.
    - [REDACTED]
    - [REDACTED]
  - Some BIS settings are not accurately described. For example:
    - [REDACTED]

### Recommendation

2.1 BIS should continue to improve its defined configuration settings in accordance with guidance in NIST SP 800-70 (as Department policy requires).

### 3. Security Control Assessment Was Not Adequate [REDACTED]

BIS' certification team assessed controls by interviewing system administrators, examining available documentation, scanning network segments to determine the composition and scope of the system, scanning [REDACTED] and [REDACTED] hosts with both network and application tools and DISA's scripts, and comparing configurations collected from [REDACTED] devices against "best practice" recommended settings. The certification team told us its overall assessment of the security status of the system relied heavily on a system penetration test it conducted.

The certification team documented the assessment results of NIST SP 800-53 controls in a spreadsheet and other documents that record the assessment objectives, methods (i.e., interview, examine, or test), objects (e.g., a person, document, or class of components), and the "actual results." In addition, the team prepared a preliminary plan of action and milestones (POA&M) that included vulnerabilities identified by technical testing (scans, scripts, etc.) and the corresponding NIST SP 800-53 controls. The certification team told us that its testing was the first phase of what it understood to be a two-phased approach to assessing the system's controls. However, the team was not called back for more testing.

- Various IT products that implement security controls were not assessed.
  - The certification team told us that absent a complete listing of hardware and installed software, it was not able to fully prepare assessment procedures for various components they eventually learned were part of the system. Significant IT products that were not assessed include:
    - application servers such as [REDACTED], [REDACTED], and [REDACTED];
    - [REDACTED];
    - operating systems: [REDACTED]; and
    - [REDACTED] (see OIG assessment in finding 6).
  - Fifty controls were not tested "due to time constraints" according to the certification team's documented results (see table 1).
    - In each case, the certification team stated, "This test should be completed during the next assessment."
    - The "test" method for assessing controls is one that is commensurate with BECCI-2's [REDACTED] security categorization according to NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.
      - However, the certification team relied on interviewing and examination methods for assessing the effectiveness of these controls.
- Assessments suffered from inadequate or inaccurate information resulting from BIS' lack of security planning (see table 2).
- In other cases, assessment procedures were not performed sufficiently to meet the assessment objectives (see table 3).

**Recommendations**

BIS should

- 3.1 assess IT products not evaluated for certification and accreditation;
- 3.2 complete assessments of controls not tested by the certification team due to time constraints;
- 3.3 ensure that control assessors are provided sufficient information resulting from improved BIS security planning processes (see finding 1); and
- 3.4 employ assessment procedures that are sufficient to meet the assessment objectives.

#### 4. Authorizing Official's Accreditation Decision Violated Department and BIS IT Security Policy and FISMA Guidance

The deputy under secretary for Industry and Security granted a "full" ATO after reviewing the BECCI-2 security accreditation package. However, the authorization letter imposed restrictions that (1) "BECCI-2 must mitigate all [high- and moderate-risk security control] deficiencies **within 180 calendar-days** from the issuance of this Letter of ATO, and confirm that the mitigations have been completed in writing to me, **or this letter is withdrawn** [emphasis added]," and (2) the status of low-risk security deficiencies be reported to him within 180 days.

- Although the system is reported in the Department's system inventory with an ATO, the restrictions included with the decision equate to an interim authorization to operate (IATO) as defined in the Department's IT security policy and NIST SP 800-37.
  - An IATO "provides authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the agency for a specified period of time."<sup>5</sup>
  - Notably, the certification team recommended an IATO based on its assessment findings and an acknowledgement of limitations in its own testing.
  - According to the Department's policy, in an ATO, risk is deemed fully acceptable and "Although **not affecting the security accreditation decision** [emphasis added], the [authorizing official] may recommend specific actions be taken by the system owner to reduce or eliminate identified vulnerabilities, where it is cost effective to do so."
    - However, the restrictions in BECCI-2's authorization letter were conditions affecting the accreditation decision—high- and moderate-risk deficiencies in controls had to be remediated in 180 days or "this letter is withdrawn."
  - BIS' actions post-ATO have reaffirmed the actual status as an IATO.
    - On April 1, 2009, the BECCI-2 system owner requested "an extension to the Authorization to Operate" for 6 months in order to complete remediation of the vulnerabilities. The memo indicated that all high-risk vulnerabilities had been "fully addressed."
      - However, some high-risk deficiencies were not remediated until April 6, 2009, after we informed BIS that high-risk deficiencies described in the executive summary of the security assessment report had not been addressed.
        - Moderate-risk deficiencies were not remediated in the 180 days following the ATO.
        - Authorizing official's granting of the 6-month extension illustrates the perceived "greater risk to the agency for a specified period of time" that is consistent with an IATO as defined under the Department's policy and FISMA's guidance.

<sup>5</sup> See U.S. Department of Commerce, *IT Security Program Policy and Minimum Implementation Standards*, Revised June 30, 2005, Section 6.7.1, 59.

- BIS policy required a Denial of ATO and does not permit an IATO because such a decision would potentially result in additional oversight by OMB. This inappropriate rationale is stated in BIS IT policy:

Although conceptually there is a third potential accreditation decision, **Interim Authorization to Operate (IATO), this is not acceptable as a matter of BIS policy because this status is not acceptable to OMB** [emphasis added]. OMB has determined that an information system is not accredited during the period of limited authorization to operate, and [does] not satisfy criteria for a well-managed investment. **Investments for systems with an IATO status are historically assigned to the OMB watch list** [emphasis added].

**Therefore, all BIS systems which might be considered as IATO systems are instead assigned to the Denial of ATO category** [emphasis added].<sup>6</sup>

- While systems operating under an IATO are not counted as accredited under the agency's FISMA scorecard, an IATO is an option under NIST SP 800-37.
- Additional oversight by the Department and OMB may have been inappropriately avoided.
  - A by-product of BIS granting an ATO (rather than an IATO or Denial of ATO) is that the Department and OMB were precluded from identifying this system as one that potentially requires greater attention from senior management.
    - An ATO "with restrictions" is not separately reported; BECCI-2 is counted as an ATO in the Department's system inventory and FISMA's report to OMB.

## Recommendations

BIS should

- 4.1 revise its policy for accreditation decisions to comply with Department policy and FISMA; and
- 4.2 follow its (revised) policy for future accreditation decisions.

<sup>6</sup> Bureau of Industry and Security, November 2007. *IT Security Program Policy*, 52.



## 5. Reporting Procedures Required by Department IT Policies Were Not Followed

- BIS did not identify any proposed deviations from the mandatory practices of the Department's IT security policy and request a waiver(s) in writing through BIS' then-CIO from the Department's IT security program manager as the policy required.<sup>7</sup>
  - BIS indicated that it chose "to focus its very scarce resources on technical controls as opposed to documentation," but in doing so failed to comply with mandatory practices of the Department's IT security policy (see finding 1).
  - While BIS asserted the deviations in security planning were generally done "with the cognizance of" BIS and Department senior management, there was no formal waiver request filed with and approved by the Department's IT security program manager.
    - BIS' then-CIO told us that a waiver request had been drafted but was never submitted to the Department.
- BIS did not submit BECCI-2's POA&M to the Department's OCIO for the first quarter of FY09.
  - As a result, the status of corrective actions for this system was not properly communicated to the Department.
  - POA&M items are now entered into cyber security assessment and management tool (CSAM) and viewable by Department OCIO officials.
- BIS did not submit the BECCI-2 privacy impact assessment (PIA) to the Department's OCIO for review and approval.
  - BIS' IT security officer told us BECCI-2 was exempted from this requirement because BECCI-2 did not have a specific system of records notice.
    - However, the Department required operating units to submit all PIAs to the OCIO, whether or not there is a specific system of records notice, for review and approval to ensure compliance with the Department's IT privacy policy. The Department's current IT privacy policy, updated January 2009, now requires operating units to submit PIAs to the Director, Office of IT Policy and Planning (OITPP), to whom the Department's CIO has delegated the authority to review, approve, and publish PIAs.
  - BECCI-2's PIA did not include information for two of the additional elements required by the Department (but not by OMB).
    - Unique project identifier (UPI) from Exhibit 300 – The Department's IT privacy policy requires that PIAs include the UPI and clearly indicate the link between the system or information collection covered by the PIA and the related major information system described in OMB Exhibit 300, *Capital Asset Plan and Business Case Summary*.
    - Data Extract Log and Verify Requirement – the December 18, 2007, memorandum from the Department's CIO titled "Data Extract Log and Verify Requirement," requires operating units to document in PIAs how the log and verify requirement of OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, has been implemented for the system.

<sup>7</sup> The Department's current IT security policy, revised in March 2009, no longer requires waivers to be submitted to the Department's IT security program manager. Instead, waiver requests are to be submitted to the operating unit's CIO, while the Department's CIO has the discretion of elevating the waiver-approval process for issues that affect Department-wide security.

**Recommendations**

BIS should

5.1 comply with the waiver process as outlined in the Department's IT security policy; and

5.2 update the BECCI-2 privacy impact assessment to include all required elements and submit it to the Director of OITPP in accordance with the Department's IT privacy policy.

## 6. OIG Control Assessment Found Vulnerabilities Requiring Remediation

As part of OIG's FY09 FISMA evaluation of BECCI-2, we assessed a targeted set of system components to determine if selected security controls are properly implemented on applicable IT products. We tailored our procedures to the infrastructure's specific control implementations.

- OIG assessments identified several weaknesses in NIST SP 800-53 controls that need to be addressed. These include the following:

[REDACTED]

- Details for NIST SP 800-53 controls are listed in table 4.
- [REDACTED] vulnerabilities identified by Gold Disk are listed in table 5.
- [REDACTED] improper settings are listed in table 6.
- [REDACTED] improper settings are listed in table 7.

**Recommendation**

6.1 BIS should add the vulnerabilities we identified in tables 4-7 and the issue with quarterly vulnerability scanning described above to the system's plan of action and milestones, and remediate the vulnerabilities accordingly.

[illegible]

Table 2. Assessments Hindered by Inadequate or Inaccurate Information

Control	Certification Team Assessment (Excerpts)		OIG Comments
	Methods/Objects	[Results]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	
	[REDACTED]	[REDACTED]	
	[REDACTED]	[REDACTED]	

Table 2. Assessments Hindered by Inadequate or Inaccurate Information

Control	Certification Team Assessment (Excerpts)		OIG Comments
	Methods/Objects	[Results]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	
	[REDACTED]	[REDACTED]	
	[REDACTED]	[REDACTED]	
	[REDACTED]	[REDACTED]	

Table 2. Assessments Hindered by Inadequate or Inaccurate Information

Control	Certification Team Assessment (Excerpts)		OIG Comments
	Methods/Objects	[Results]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]



Table 3. Insufficient Assessment Procedures

Certification Team Assessment (Excerpts)						OIG Comments
Control	Assessment Objective	Method/Objects [Procedure]	Actual Results	Met?	Evidence	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 3. Insufficient Assessment Procedures

Certification Team Assessment (Excerpts)						OIG Comments
Control	Assessment Objective	Method/Objects [Procedure]	Actual Results	Met?	Evidence	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 3. Insufficient Assessment Procedures

Certification Team Assessment (Excerpts)						OIG Comments
Control	Assessment Objective	Method/Objects [Procedure]	Actual Results	Met?	Evidence	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 3. Insufficient Assessment Procedures

Certification Team Assessment (Excerpts)						OIG Comments
Control	Assessment Objective	Method/Objects [Procedure]	Actual Results	Met?	Evidence	
<b>E</b>	[REDACTED]	[REDACTED]	[REDACTED]	<b>X</b>	[REDACTED]	[REDACTED]

Table 3. Insufficient Assessment Procedures

Certification Team Assessment (Excerpts)						OIG Comments
Control	Assessment Objective	Method/Objects [Procedure]	Actual Results	Met?	Evidence	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Table 4. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	OIG Assessment Results
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]

Table 4. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	OIG Assessment Results
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Table 4. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	OIG Assessment Results
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]



Table 4. **OIG Control Assessment Results**

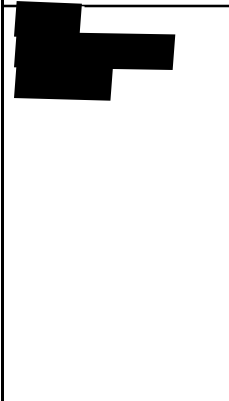

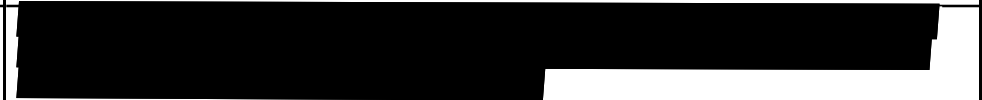



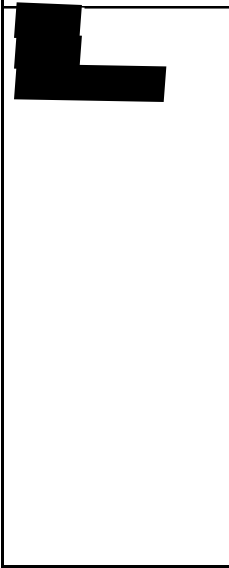
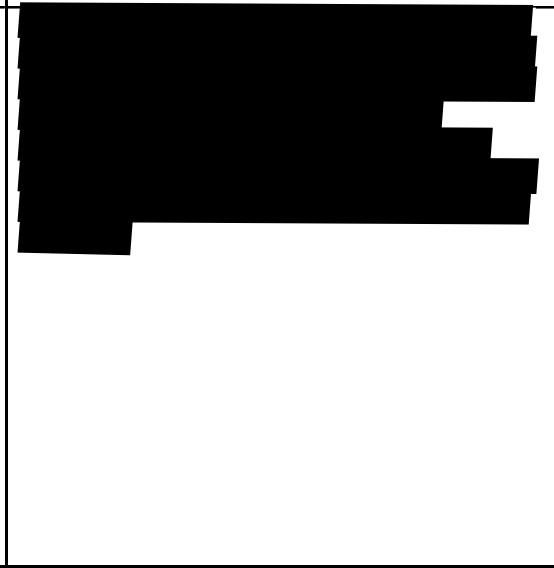




Security Control	NIST SP 800-53 Requirement	OIG Assessment Results
		
		
		
		
		
		
		
		

Table 4. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	OIG Assessment Results
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

Table 4. **OIG Control Assessment Results**

Security Control	NIST SP 800-53 Requirement	OIG Assessment Results
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]
		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
		[REDACTED]

Page 33

Page 34

Table 5. [REDACTED] Vulnerabilities Identified by DISA's Gold Disk (OIG Control Assessment)

Vulnerability Description	BIS Assertion (Full Quotation)	OIG Comments
[REDACTED]	[REDACTED]	[REDACTED]  [REDACTED]  [REDACTED]  [REDACTED] SSP implementation description for access enforcement.
[REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

Page 36

Page 37



Table 6. [REDACTED] Improper Configuration Settings (OIG Control Assessment)

Rule Name	Device	Instance	Total	OIG Comments
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	
	[REDACTED]	[REDACTED]	[REDACTED]	
	[REDACTED]	[REDACTED]	[REDACTED]	
	[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]			[REDACTED]	

Page 39

## Appendix A: Objectives, Scope, and Methodology

To meet the FY 2009 Federal Information Security Management Act of 2002 (FISMA) reporting requirements, we evaluated the BIS certification and accreditation for the Bureau Export Control Cyber Infrastructure, Version 2 (BECCI-2).

Security certification and accreditation packages contain three elements, which form the basis of an authorizing official's decision to accredit a system:

- The **system security plan** describes the system, the requirements for security controls, and the details of how the requirements are being met. The security plan provides a basis for assessing security controls and also includes other documents such as the system risk assessment and contingency plan, per Department policy.
- The **security assessment report** presents the results of the security assessment and recommendations for correcting control deficiencies or mitigating identified vulnerabilities. This report is prepared by the certification agent.
- The **plan of action & milestones (POA&M)** is based on the results of the security assessment. It documents actions taken or planned to address remaining vulnerabilities in the system.

The Department's *IT Security Program Policy and Minimum Implementation Standards* requires that C&A packages contain a certification documentation package of supporting evidence of the adequacy of the security assessment. Two important components of this documentation are

- the **certification test plan**, which documents the scope and procedures for testing (assessing) the system's ability to meet control requirements; and
- the **certification test results**, which is the raw data collected during the assessment.

To evaluate the certification and accreditation, we reviewed all components of the C&A package and interviewed BIS staff to clarify any apparent omissions or discrepancies in the documentation and gain further insight on the extent of the security assessment. We evaluated the security plan and assessment results for applicable security controls and will give substantial weight to the evidence that supports the rigor of the security assessment when reporting our findings to OMB.

In addition, we performed our own assessment of a targeted selection of controls (see appendix B). We conducted our assessment using a subset of procedures from NIST SP 800-53A, which we tailored to BECCI-2's specific control implementations. We did not attempt to perform a complete assessment of each control; instead we chose to focus on specific technical and operational elements.

We assessed controls on key classes of IT components, choosing a targeted set of components from each class that would allow for direct comparison with BIS' certification test results. We assessed configuration settings on [REDACTED]

[REDACTED] We looked at controls implemented on [REDACTED] and network-addressable [REDACTED]. We also assessed aspects of controls implemented by firewalls (specifically the rule sets) [REDACTED].

[REDACTED] We also performed vulnerability scanning using Nessus.

Our assessment included the following activities:

- extraction, examination, and verification of system configurations
- execution of scripts and manual checklists
- examination of system logs
- review of account management procedures
- vulnerability scanning of network-addressable components
- examination/analysis of security plan descriptions, including related policy and procedure documents
- interviews of appropriate BIS personnel

Our assessment was limited in scope and should not be interpreted as the comprehensive review that a security certification for a [REDACTED] system would require. It gave us direct assurance of the status of select aspects of important system controls and provided meaningful comparison to BIS' security certification.

We reviewed the BECCI-2 privacy impact assessment as part of privacy reporting requirements included in our annual FISMA report to OMB.

We used the following review criteria:

- Federal Information Security Management Act of 2002 (FISMA)
- U.S. Department of Commerce *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005
- NIST Federal Information Processing Standards (FIPS)
  - Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
  - Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications:
  - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - 800-53, *Recommended Security Controls for Federal Information Systems*
  - 800-53, *A Guide for Assessing the Security Controls in Federal Information Systems*
  - 800-70, *Security Configuration Checklists Program for IT Products*
  - 800-115, *Technical Guide to Information Security Testing and Assessment*

We conducted our evaluation in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections* (revised January 2005), issued by the President's Council on Integrity and Efficiency.

## **Appendix B: NIST SP 800-53 Security Controls Assessed by OIG**

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-7 Unsuccessful Login Attempts
- AC-8 System Use Notification
- AC-11 Session Lock
- AU-2 Auditable Events
- AU-6 Audit Monitoring, Analysis, and Reporting
- AU-8 Time Stamps
- AU-9 Protection of Audit Information
- AU-11 Audit Record Retention
- CM-6 Configuration Settings
- CM-7 Least Functionality
- IA-2 User Identification and Authentication
- IA-3 Device Identification and Authentication
- IA-5 Authenticator Management
- PL-4 Rules of Behavior
- SC-7 Boundary Protection
- SC-18 Mobile Code
- SI-2 Flaw Remediation
- SI-3 Malicious Code Protection
- SI-4 Information System Monitoring Tools and Techniques
- SI-7 Software and Information Integrity



SEP 25 2009

MEMORANDUM FOR ALLEN CRAWLEY

Assistant Inspector General  
for Systems Acquisition and IT Security

FROM:

Daniel O. Hill *[Signature]*  
Acting Under Secretary

SUBJECT:

Draft Inspection Report No. OSE-19575: *FY2009 FISMA  
Assessment of Bureau Export Control Cyber Infrastructure,  
Version 2 (BECCI-2)*

Thank you for the opportunity to comment on the above-referenced draft OIG Report. The OIG FY 2009 FISMA Assessment of BECCI-2 provides the BIS Office of the Chief Information Officer (OCIO) with valuable information that will be incorporated into system security planning, configuration management and monitoring. The findings and recommendations from the draft OIG Inspection Report have been reviewed and BIS does not dispute the findings.

To ensure compliance moving forward, one of the OCIO's major objectives for FY 2010 is a complete and approved C&A for all our systems, especially [REDACTED] infrastructure. In anticipation of the full FY 2010 President's Request, the BIS OCIO has begun efforts to improve our C&A documentation, IT workforce skills and overall FISMA responsibilities.

If you have any questions comments on our response, please contact Eddie Donnell, BIS' Acting Chief Information Officer, at (202) 482-4296.

cc: Suzanne Hilding,  
Chief Information Officer

