U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

Bureau of Economic Analysis

FY 2008 FISMA Assessment of BEA Estimation Information Technology System (BEA-015)

Final Inspection Report No. OSE-19001/September 2008

FOR PUBLIC RELEASE

Office of Systems Evaluation

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

SEP 22 2008

MEMORANDUM FOR: J. Steven Landefeld
Director
Bureau of Economic Analysis

Judith J. Gordon

FROM: Judith J. Gordon
Assistant Inspector General for Audit and Evaluation

SUBJECT: Bureau of Economic Analysis
FY 2008 FISMA Assessment of BEA Estimation Information Technology System (BEA-015)
Final Inspection Report No. OSE-19001

This report presents the results of our Federal Information Security Management Act (FISMA) review of the BEA Estimation Information Technology System certification and accreditation. We found that while the system security plan provided an adequate basis to conduct the security certification, BEA needs to improve its security control assessments to assure that controls are implemented as intended. We also found that BEA needs to correct its process for tracking and reporting security weaknesses as required by Department policy and OMB's FISMA guidance. Finally, we performed our own assessment of selected BEA security controls and found weaknesses in those controls that BEA's security certification did not.

In response to our draft report, BEA with one exception did not specifically indicate whether it agreed with our findings and the corrective actions described are not fully responsive to our recommendations. BEA's response is summarized in the appropriate sections of the report and included in it entirety as appendix B.

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. The plan should be in the form of plans of action and milestones (POA&Ms) 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) 482-2754 or Allen Crawley, Deputy Assistant Inspector General for Systems Evaluation at (202) 482-1855.

Attachment

cc: Suzanne Hilding, Chief Information Officer, U.S. Department of Commerce
Brian Callahan, Chief Information Officer, Bureau of Economic Analysis

Listing of Abbreviated Terms & Acronyms

BEA	Bureau of Economic Analysis
BEA-EITS	BEA-Estimation Information Technology System
C&A	Certification and Accreditation
CIO	Chief Information Officer
DISA	Defense Information Systems Agency
DOC	Department of Commerce
FISMA	Federal Information Security Management Act of 2002
IT	Information Technology
ITSO	Information Technology Security Officer
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SSP	System Security Plan
ST&E	Security Test and Evaluation

Synopsis of Findings

- System security plan provided an adequate basis to conduct the security certification.

- Security certification lacked credible supporting evidence for technical security control assessments.

- Vulnerabilities were not included in the security assessment report or identified in POA&Ms.

- OIG assessment of selected security controls found significant weaknesses not identified by the BEA security certification.

Conclusions

- BEA needs to improve security control assessments to assure that controls are implemented correctly, operating as intended, and meeting the security requirements for the system.

- The bureau should correct its process for tracking security weaknesses in POA&Ms as required by Department policy and FISMA guidance.

Summary of BEA Response

BEA's response to our draft report included a memorandum from the director with a brief discussion of each finding and a memorandum from the CIO describing actions taken since our review, discussion of some of the issues we found, and a table of action items addressing each of our recommendations.

The CIO described actions completed since our review ended: the agency has improved its continuous monitoring program, with the system's authorizing official reviewing results; had independent contractors perform a network penetration test; and developed a secure configuration standard for Windows [redacted] servers after implementing the federal desktop core configuration for its Windows [redacted] desktops.

In regard to BEA's work developing secure configuration standards, the CIO described its risk-based approach for implementing the standards on system components. The bureau, intending to configure its most valuable assets first and minimize disruption to its core processes of producing statistics, is only now configuring its less sensitive servers. The risk-based approach was said to be "reflected in the [OIG] report where it is noted that some servers did not conform to our standard." The need for completing this work has now been added to the system POA&M in line with one of our recommendations.

The CIO also makes the point that BEA is a small operating unit and depends on private contractors to provide independent security control assessments. While BEA exercised care in its selection, the contractors "have not met the documentation expectations of the OIG."

The portions of the response applicable to our specific findings are described in the body of this report along with OIG comments. The bureau's response is included in its entirety as appendix B.

OIG Comments

BEA did not specifically indicate whether it agreed with our findings (with one exception), and the corrective actions described are not fully responsive to our recommendations. The bureau did indicate its intention to use our recommendations to improve BEA information security.

In its response, BEA appears to view the deficiencies we identified as primarily a documentation issue. We disagree. We attribute our finding on the lack credible supporting evidence for technical security control assessments to the inadequacy of the assessments themselves. This is supported by OIG's assessment of controls, which while limited, found significant deficiencies in critical components.

BEA's risk-based approach to implementing secure configuration settings was described in the status of action items addressing two of our recommendations. In both cases, the discussion is not responsive to our recommendations (see OIG comments in body of report). While a risk-based approach may be entirely appropriate, we disagree with BEA's assertion that it explains why we found insecure settings in the components we assessed. Some security control deficiencies were present in a certain subset of (noncritical) servers, but many secure configuration settings were missing across the full spectrum of components we examined, including components that process sensitive core data. BEA's own secure configuration standard for Windows showed that many settings had not yet been implemented in its two main network domains, and made no distinction between more and less valuable assets in those domains. However, BEA's C&A process did not raise this as a risk or add appropriate actions to the system's POA&M.

Introduction

BEA-015, BEA Estimation Information Technology System (BEA-EITS), encompasses all of BEA's information technology in support of its mission to promote a better understanding of the U.S. economy by providing the most timely, relevant, and accurate economic accounts data in an objective and cost-effective manner. The bureau, "produces some of the most closely watched U.S. economic statistics that influence critical financial decisions made by governments, businesses, and households."[1] BEA-EITS is utilized in BEA's core business processes: data collection; analysis, tabulation, and estimation; and data dissemination.

BEA has categorized BEA-EITS [redacted] [redacted]mpact system, which means a security breach could be expected to [redacted] effect on organizational operations and assets, or individuals.

The system is made up of a LAN infrastructure that includes web and remote access segments among others. Network components (primarily Cisco firewalls, routers, and switches) regulate the flow of internal and external communications. Windows servers process BEA information and perform key security services such as identification/authentication and access control. BEA's internal users access the system via Windows workstations and laptops. BEA also provides public access to data via the Web. The system has a number of other components (such as remote access servers, [redacted] servers, storage area network) and applications (e-mail server, desktop office automation software, VPN clients, databases, proprietary applications).

[1] BEA. *Mission, Vision, Values* [Online]. www.bea.gov/about/mission.htm (accessed May 30, 2008).

Findings and Recommendations

1. System Security Plan Provided an Adequate Basis to Conduct the Security Certification

- The system description correctly represented the system components and defined the accreditation boundary.
  - Component listing was accurate.
  - System boundaries and interconnections were defined.

- In general, the security plan sufficiently addressed all applicable aspects of the required controls.
  - In the summer of 2006, OIG reviewed this system's C&A package and found configuration settings (CM-6) for IT products had not been defined. A review of the current CM-6 control description in the security plan showed significant improvement—BEA has defined settings by adapting industry-defined secure configuration settings baselines for significant IT products implemented on the system.
    - A weakness we found was that the baseline [redacted] (a Microsoft [redacted]) does not describe the rationale for deviating from the DISA benchmark from which BEA's baseline is derived. In addition, [redacted] DISA benchmark used by BEA is now out of date. DISA has published a new, more extensive benchmark.

Recommendations

BEA should

1.1 document secure configuration baselines with its rationale for deviating from the benchmarks, as appropriate; and

1.2 update its secure configuration baseline for IIS using the most current DISA benchmark available.

BEA Response

BEA noted the extensive work the bureau has done in developing the system security plan.. With respect to our first recommendation (1.1), BEA described actions it has taken in developing a standard configuration for Windows[redacted] servers. The bureau explained that it used a risk-based approach to implement configuration settings on its more valuable servers first and was currently securely configuring servers carrying less sensitive information. BEA indicated that it has updated its secure configuration baseline[redacted] [redacted]using the most current DISA benchmark (in response to recommendation 1.2).

OIG Comment

We appreciate BEA's efforts to improve security planning. However, the bureau was not responsive to recommendation 1.1 to document secure configuration baselines with appropriate rationale. Instead, the response is apparently addressing some aspects of finding 4 below. Recommendation 1.2 stemmed from our finding that BEA's secure baseline [redacted] did not describe the rationale for defining settings that deviated from DISA-recommended settings. This type of documentation is recommended in NIST guidance as a means of recording the tailoring of baselines to reflect IT security policy and operational needs, and should be a normal part of defining all of the system's secure configuration baselines—including the baseline for Windows [redacted] servers that BEA is currently revising and its updated baseline [redacted].

2. Security Certification Lacked Credible Supporting Evidence for Technical Security Control Assessments

In FY06, OIG reviewed BEA-EITS' C&A as part of the annual FISMA evaluation. We identified significant weaknesses in the security control assessments, specifically:

- Procedures to assess security controls were not applied to all the network components where the controls were required to be implemented.
- Assessment results did not provide a basis for evaluating the adequacy of security controls.
- Assessments of technical controls were only based on policy review and interview.
- Frequently the assessments simply restated the control requirement with no meaningful information about the actual security control implementation or supporting evidence.

The FY07 security certification showed some improvement—in particular, some of the required operational and management security control assessments were supported by evidence. However, we still found significant control assessment issues that indicate the security certification did not credibly identify the remaining vulnerabilities in the system. We focused on assessments that called for an examination or test of security controls implemented on system components (technical assessments).

- Of the 71 technical assessments, 55 cases (77%) lacked supporting evidence or the assessment activity was inappropriate.
    - 44 technical assessments were not supported by artifacts or other evidence to validate the results. (See table 1 for examples.)
    - In 11 of the remaining 27 cases, the evidence indicated the assessment activity was inappropriate or incomplete. (See table 2 for examples.)

- As in FY06, the certifier's assessment procedures and results lacked specific information, such as which components were assessed and actual settings examined. (See table 3 for examples.)
    - Results were typically just restatements of generally worded procedures.
    - Assessments were either exactly the same as the FY06 assessments or had just minor alterations.

- The C&A package included two sets of results, one labeled "certifiers results" and the other "ST&E results." The assessment procedures used in both were the same or similar; however, the results were different in several cases. BEA told us that the certifier's results were the definitive results but also stressed that both assessments should be considered. (See table 4.)

Recommendations

BEA should ensure that

2.1 all control assessments are supported by credible evidence to validate the assessment results;

2.2 evidence shows that all applicable aspects of a control and an appropriate sample of components implementing it have been assessed; and

2.3 assessment procedures and results include specific information about the implementation of the control and the steps taken to assess it.

BEA Response

BEA did not specifically indicate if it agreed with this finding but explained that the private sector contractors who performed the security certification were chosen in large part due to “past successful performance.” The bureau indicated that the contractors did not meet “the documentation expectations of the OIG,” and that “what is considered acceptable documentation varies greatly across agencies.”

The bureau described the steps it is taking in its continuous monitoring to address our recommendations. The authorizing official is reviewing control assessments for technical security control families as they are completed. The bureau’s CIO indicates that “test results are thoroughly documented with clear and appropriate artifacts,” and that BEA “would welcome a review of this completed documentation to ensure that it meets OIG expectations.” The bureau emphasized the promptness of its process for reviewing residual risks identified by this testing.

OIG Comments

BEA’s response suggests that the problems we identified were mostly attributable to poor documentation of testing. On the contrary, we view our findings as evidence of inadequate security control assessments. Our own control assessments, documented in finding 4 below, support this position.

Adequate documentation is the byproduct of comprehensive control assessments required for a security certification. Further, such documentation is not an “OIG expectation.” The assessment process described in NIST SP 800-53A, *Guide for Assessing the Security Controls in Information Systems* states, “Security assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits…” BEA’s security assessments included much paperwork but little evidence of tailored and scoped control assessment procedures and results that gave credible confirmation of the status of controls.

While BEA attributes the problems to contractor performance, the bureau has the responsibility of overseeing the contractors’ work for appropriate quality. Indeed, in our review, BEA staff told us they worked closely with the contractors and reviewed control assessments in real time.

BEA’s response does not describe specific steps it will take to ensure each recommendation is implemented, and instead emphasizes its review process. We reiterate the need for BEA to ensure that (1) control assessments are supported by credible evidence, (2) all applicable aspects of a control are assessed on appropriate samples of components, and (3) procedures and results include specific information about control implementations.

With regard to OIG reviewing continuous monitoring control assessments, we have issued a data call for this information and will consider it in our annual FISMA report to OMB.

3. Vulnerabilities Were Not Included in the Security Assessment Report or Identified in POA&Ms

- Significant vulnerabilities discovered during C&A were not identified in the required security assessment report and vulnerabilities requiring mitigation were not tracked in a POA&M.
  - Windows configuration vulnerabilities were not described in the security assessment report and are currently being tracked outside the required POA&M process, which prevents mandated oversight by responsible Department and OMB officials.
    - BEA is tracking these vulnerabilities, which are unimplemented secure configuration settings defined in BEA's Windows Security Standard, through an internal process.
    - These vulnerabilities were identified more than 1 year ago, but BEA still has not scheduled mitigation.
  - BEA's CIO told us that he does not consider many of the unimplemented secure configuration settings for Windows to be vulnerabilities, the settings may never be implemented, and the secure configuration baseline may be revised as a result. However, this acceptance of risk was not documented in the C&A package. In addition, OIG's assessment of controls found that the implementation of secure settings on servers was less complete than BEA's internal tracking indicates.

Recommendations

BEA should

3.1 comply with Department policy and guidance in tracking and correcting system security deficiencies;

3.2 create POA&Ms to address the Windows vulnerabilities described above;

3.3 explain vulnerabilities in security assessment reports according to guidance found in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; and

3.4 clearly articulate in the C&A package the vulnerabilities for which the bureau is accepting risk. Unimplemented secure configuration settings should be addressed in the security assessment report as well as the accreditation decision letter. If BEA chooses to redefine its secure baseline, that document should be updated with appropriate risk rationale.

BEA Response

BEA stated that it carefully tracks security weaknesses, but agreed that it had not done so properly through the use of POA&Ms. The bureau indicated that it would be listing on POA&Ms vulnerabilities that could not be mitigated quickly. It has recently added items related to secure configuration of Windows servers and the standard web browser to its system POA&M.

Security assessment reports are being prepared for technical security controls reviewed in the continuous monitoring program. These reports are reviewed by BEA's authorizing official (the CIO) and risk is either accepted or corrective actions prescribed. BEA is redefining its secure configuration for Windows [redacted] servers and these settings must be thoroughly tested before being implemented in its production environment. BEA's risk-based approach was to implement settings in its most valuable assets first and minimize the potential for disruption in its critical processes. This approach explains why OIG found some servers did not conform to the BEA secure baseline. A weakness related to completing implementation of secure configurations has been added to the system POA&M.

OIG Comments

BEA's corrective actions are generally responsive to our recommendations. However, the bureau did not speak to the portion of recommendation 3.4 that suggests appropriate risk rationale be included in secure configuration baselines BEA chooses to redefine. A related recommendation in finding one (1.2) was also not addressed by the BEA response, so we are concerned BEA may not adequately define its secure configuration baselines.

The Windows configuration vulnerabilities referred to in this finding were not limited to less sensitive servers. Our finding related to specific settings that according to BEA's own internal tracking had not been implemented in its production and web domains. Together these components encompass the vast majority of BEA servers—including those performing the most critical operations referred to in its risk-based approach.

4. OIG Assessment of Selected Security Controls Found Significant Weaknesses Not Identified by the BEA Security Certification

As part of the OIG's FY08 FISMA evaluation of BEA-EITS, we assessed a targeted set of system components to determine if selected security controls are properly implemented and whether related system vulnerabilities were identified by BEA's security certification. We tailored our procedures to the specific control implementations of BEA-EITS. This tailoring is a necessary part of assessing controls adequately and is a crucial component of NIST guidance. The results follow from the steps we took to assess the control, include (or reference) our analysis, and cite specific supporting evidence. (See appendix C.) The assessments, along with the supporting evidence, are transparent, clearly depicting the status of the controls in order to effectively inform those who manage risk to agency operations, agency assets, and individuals.

- We found weaknesses in the technical implementation of security controls that were not identified by the BEA security certification. (See table 5.) Some of our significant findings are as follows:
    - o [redacted]

Recommendations

BEA should ensure that

4.1 the deficiencies we identified are added to the system's POA&M and remediated in a timely manner; and

4.2 control assessments are improved through tailored procedures and well-supported results which provide a transparent view of the status of controls.

BEA Response

BEA stated that it continuously monitors the effectiveness of security controls. BEA chose to devote its scarce resources toward its first priority—the protection of critical market-sensitive and company-confidential data. The bureau stated that it understands the importance of protecting the entire system and is expanding the scope of its continuous monitoring program to include all system components.

The bureau indicated that most of the items OIG identified in this finding have been remediated and those requiring longer term efforts have been added to the system POA&M. It stated that it could not replicate the finding of out-of-date virus signatures and that two issues we identified in Cisco components were not accurate.

In response to our recommendation to ensure improved control assessments, BEA reiterated that security assessment reports were being prepared for each control family assessed in its continuous monitoring, the authorizing official accepts risks or prescribes corrective actions, and the system POA&M will include deficiencies that cannot be corrected promptly.

OIG Comments

BEA corrective actions are responsive to our recommendation to add the deficiencies we identified to the system's POA&M and remediate them in a timely manner. The bureau suggests that most deficiencies have already been corrected and therefore will not be added to the POA&M. In those cases, the remediation should be verified through appropriate control testing—which can be done as part of the continuous monitoring. With respect to the out-of-date virus signatures, BEA staff and OIG jointly concluded that the signatures had been out-of-date at the time of our testing, but had since been updated and were current as of a meeting held immediately after our exit conference on May 8, 2008. Therefore, it was not a deficiency we expected BEA to add to its POA&M.

BEA was not entirely responsive to our recommendation to ensure that control assessments were improved through tailored procedures and well-supported results (4.2). Rather than addressing tailoring of assessment procedures, the bureau emphasized its security assessment reports (results) and in response to an earlier recommendation (2.1) indicated that more current assessment results from its contractor were thoroughly documented with clear and appropriate artifacts.

Table 1: Examples of Technical Examinations or Tests Not Supported by Evidence.

Control	BEA's C&A Package			OIG Comments
	Procedural Step	**Certifier's Results (full quotation)**	**ST&E Results (full quotation)**	
IA-3 Device Identification and Authentication	IA-3.1 **Examine** BEA's records or documents and information system configuration settings to determine if the system uses either shared known information or BEA's authentication solution to identify and authenticate devices on local and/or wide-area networks.	[redacted]	[redacted]	There is no evidence that Nmap was used to assess this control or even what relation Nmap has to the implementation of this control. Specific settings examined are not identified ("Nmap and VPN configurations" does not identify which specific settings pertain to Device Identification and Authentication—and it is unlikely that either would have settings relevant to IA-3). The statement "tested an IT system for compliance," in the ST&E results gives no specifics as to what the test actually consisted of (i.e., how was the test performed?) or what components were tested. There are no artifacts or other evidence of such a test. The procedural step (taken from NIST SP 800-53A, Second Public Draft) was not tailored for the specific control implementations in the system. (For example, the assessment did not document which specific settings were examined or how they pertain to IA-3 or, what the data collection method was.) Neither set of results reflects the actions called for in the procedural step. We also note that the procedural step and certifier's result are the same in the FY06 and FY07 packages.
SC-14 Public Access Protections	SC-14.2 Test the publicly available information system by attempting to alter protected information using a public account to determine if access is limited in order to preserve the integrity of the information and the applications.	[redacted]	[redacted].	There is no evidence that a penetration test took place on the system. BEA staff told us that no such test took place and could not explain why the certifier claimed one had. The procedural step and certifier's results are the same from FY06 to FY07. ST&E results suggest the need for additional assessment using commercial products to assess the control but provide no evidence that the control is in place or that the additional assessment was conducted. The statement, "Technical controls seem to stop this type of activity" is not supported by any specifics or evidence. There is no basis for the conclusion: "Low – Met all requirements to satisfy this control."

Table 1: Examples of Technical Examinations or Tests Not Supported by Evidence.

Control	BEA's C&A Package			OIG Comments
	Procedural Step	**Certifier's Results (full quotation)**	**ST&E Results (full quotation)**	
AU-9 Protection of Audit Information	AU-9.1 **Examine the information system configuration** to determine if the system protects audit information and audit tools from unauthorized access, modification, and deletion.	[redacted]	[redacted]	Certifier's results do not identify which specific settings were examined or what was specifically found. The statement "Audit logs…are restricted by file permissions…These are limited to Domain and [redacted] database administrators" is identical to the security plan description for this control. There are neither evidence nor artifacts that validate what the certifier claimed to have examined. ST&E efforts did not actually follow the procedural step. Rather, they rely on document review and state that the control should be in place based on system descriptions. This was not a valid technical control assessment.

Table 2: Examples of Control Assessments With Inappropriate or Incomplete Evidence.

Control	BEA's C&A Package			OIG Comments
	Procedural Step	Certifier's Results (full quotation)	Assessment Evidence	
SA-7 User-Installed Software.	SA-7.5 Test network traffic on the information system to determine if prohibited software is installed and operational by utilizing a network packet analyzer. (Note: Applications tend to communicate on known ports and/or have signature traffic patterns and common packets.)	[redacted]	[redacted]	While there was evidence that some sort of packet capture was performed, the file only showed five packets, which is not enough to assert that no unauthorized software is operating on the system. Neither the results nor the evidence was specific about actual procedures employed for the packet capture (such as at what point on the network the traffic was "sniffed," whether a filter was used to look for specific protocols, what protocols were observed, etc.).
AU-3 Content of Audit Records	AU-3.2 Test the content of audit records by attempting to perform actions that are configured to generate audit records to determine if the audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	[redacted]	[redacted].	There are two logs with time stamps from 5/08/07 but neither appear to be Windows event logs as suggested by "security, application, and system" described in the results. Besides being in the AU artifacts folder, there is nothing to tie them to this procedure. The procedural step calls for an event to be generated followed by an examination of the logs to see if the event can be reconstructed and identified. It is unclear if the two logs are the actual logs used in the test since the procedures do not state what the event was or which components were meant to capture the event, and the logs were not analyzed. The fact there are logs in the certification package that have a time stamp for the same day as the procedure is incidental.
CM-7 Least Functionality	CM -7.2 Test the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted.	[redacted]	[redacted]	Actual output from external telnet requests was included demonstrating that the certifier tested one prohibited protocol on one component. However, the assessment was not comprehensive. Note: The ST&E results state that the assessment was done with vulnerability scanning, which would be a more complete approach. BEA stated that the certifier's results were definitive and would incorporate the ST&E results. However, there was little evidence that the certifier had used the ST&E results, as demonstrated by the different method the certifier chose to assess the control.

Table 3: Examples of Assessment Procedures and Results Without Specific Information.

Control	BEA's Original (FY06) Procedural Step/Result (full quotation)	OIG Comments (in FY06)	BEA's FY07 Procedural Step/Result (full quotation, with changes to the FY06 assessment results in bold)	OIG Comments
AU-9 Protection of Audit Information	AU-9.2 Test the protection of audit information and audit tools from unauthorized access, modification, and deletion by attempting to gain unauthorized access, modify, and delete audit information. Assessment Result: The certifier tested the protection of audit information and audit tools from unauthorized access, modification, and deletion by attempting to gain unauthorized access, modify and delete audit information.	[redacted]	[redacted]	Assessment results do not provide a basis for evaluating the adequacy of the security control. It is unclear what was done to test the control or on which components the control was assessed. The only evidence in the certification package for this date was a log showing a failed logon attempt to a [redacted] switch—demonstrating that the system logs failed access attempts. The test did not address the control requirement that the system protect audit information and audit tools from unauthorized access. BEA audit data, in addition to being stored on network devices, is stored on SYSLOG servers and Windows components.
IA-2 User Identification and Authentication	IA-2.3 Test the information system to determine if passwords, tokens, or biometrics meet Level 2, 3, or 4 requirements consistent with NIST Special Publication 800-63. Assessment Result: The certifier tested the information system and has determined that passwords, tokens, or meet Level 2, 3, or 4 requirements consistent with NIST Special Publication 800-63.	[redacted]	[redacted]	The assessment does not describe the specific test(s) performed. While the results describe generic component classes and one specific application, there is no supporting evidence in the certifier's assessment artifacts for IA. Note: The default domain policy is included in a separate part of the C&A package and includes password policy settings, but this would only work for Windows components and is not evidence of a test, but instead a configuration examination (if in fact the password policy was examined). There is no evidence of [redacted] password settings, application settings, or [redacted] device settings.
AC-3 Access	AC-3.2 Examine access control mechanisms to determine if the	Controls were assessed by	[redacted]	The testing mentioned in the results is not detailed to any degree and does not

Table 3: Examples of Assessment Procedures and Results Without Specific Information.

Control	BEA's Original (FY06) Procedural Step/Result (full quotation)	OIG Comments (in FY06)	BEA's FY07 Procedural Step/Result (full quotation, with changes to the FY06 assessment results in bold)	OIG Comments
Enforcement	information system is configured to implement the organization's access control policy. Assessment Result: The certifier examined the BEA IT Security Plan, BEA Standard Operating Procedure 50-18A:Network Users Creation Procedure, BEA Remote Access Security Standard, BEA Standard Operating Procedure 20.6 (Revision 3) Employee Accountability Clearance, BEA Standard Operating Procedure 20.17 (Revision 5): Security Standards and Authorizations, Technical Requirements to Remote Access to BEA Information Technology Resources, BEA Local Area Network Security Policies, BEA Standard Operating Procedure 80.2: Password Policy for Information Technology Resources Within the BEA Network, BEA IT Remote Access Security Work Agreement, BEA Configuration Management Policy, BEA's System Change Request Process and the DOC IT Security Program Policy and Minimum Implementation Standards (June 2005) chapter 17, section 17.4. Based upon the information obtained by examining the documentation, the certifier has determined that BEA's access control mechanisms for the information system are configured to implement the BEA access control policy.	[redacted]	[redacted]	match the procedural step to examine access control mechanisms. There is no evidence to support a test or examination of access control mechanisms to determine if BEA's access control policy is correctly implemented. There is some discussion of Active Directory in the ST&E result. However, the discussion pertains to password length (IA-2), not access enforcement. There is no evidence in the package that the access enforcement mechanisms for workstations, network devices, databases, and applications were all examined or tested as claimed by the certifier. Specific components tested are not identified. There is no additional analysis by the certification team to identify if it found any deficiencies or the basis for its assertion that access control mechanisms "are configured to implement the BEA access control policy."

Table 4: Different Results in Certifier's and ST&E Assessments.

Control	BEA's C&A Package			OIG Comments
	Security Plan Description (full quotation)	Certifier's Results (full quotation)	ST&E Assessment Results (full quotation, staff names removed)	
AC-14 Permitted Actions Without Identification or Authentication	BEA does not permit access to the Local Area Network to perform any actions on the BEA-EITS system without identification or authentication.	[redacted].	[redacted] [redacted].	There is no evidence of a test as described in certifier's results. Since the test description lacks specifics, there is little assurance that requirement is met. The ST&E results conclude there is no need to test the control. However, simply prohibiting access to the system in policy does not verify that there are no accounts such as guest accounts that do not require a password. The assessment should validate this in the control implementation.
AC-18 Wireless Access Restrictions	BEA has no internal wireless access points to the BEA network, except Blackberry. BEA's Enhancement Control Implementation: All wireless traffic to and from the BES server and the Blackberry handheld devices is Triple DES (3DES) encrypted	[redacted]	[redacted]	Certifier's results state: "BEA does not allow wireless access," but the security plan describes controls for Blackberry implementation. The ST&E asserts [redacted] server configuration settings were examined but there is no supporting evidence in the package. Since the results do not specify which specific settings, there is little assurance the control was properly assessed.
AC-2 Account Management	All BEA accounts have passwords that expire in 90 days. While the account is not disabled as required by this control, it is effectively made unavailable after 90 days until an administrator changes the password.	[redacted]	[redacted]	The ST&E results found that inactive accounts are not automatically disabled. Yet the certifier's results, which BEA holds as definitive, state that the system does automatically disable inactive accounts.

Table 5: Summary Comparison of Results from OIG Control Assessment and BEA Security Certification.

Control	Control Requirement	BEA's Security Assessment Report (SAR)	OIG Assessment Result (Summary)
AC-2 Account Management	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*]. Control enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary and emergency accounts after: Not Applicable. (3) The information system automatically disables inactive accounts after 90 days. (4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.	BEA SAR states: [redacted] [redacted]	An examination of user accounts on BEA-EITS verified that BEA is following its procedures for establishing, activating, modifying, disabling, and removing accounts. Assessments revealed that the BEA system has the tools and capabilities in place to regularly review accounts but there was no evidence to support accounts are reviewed weekly as required by BEA policy. (Assessments in the ST&E indicate that it is done monthly rather than weekly as required by policy) While the security plan states that BEA does not create temporary or emergency accounts, BEA's account management policy states that temporary accounts are issued to employees such as interns. As noted in the SAR and SSP the BEA system is not configured to automatically disable accounts after an organizationally-defined period. As a compensating control BEA states that password expiration will cause the account to be locked until it is reset by an administrator. We assessed the described compensating control (for enhancement 3) and verified that in fact the user is locked out when the password is expired.
AC-3 Access Enforcement	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	[redacted]	A review of security groups for BEA operating divisions revealed that division security groups allow for access enforcement within the information system. However, a review of three user accounts and their assigned rights showed that one account was not added to the proper security groups according to the user's account authorization documentation.

Table 5: Summary Comparison of Results from OIG Control Assessment and BEA Security Certification.

Control	Control Requirement	BEA's Security Assessment Report (SAR)	OIG Assessment Result (Summary)
AC-7 Unsuccessful Login Attempts	The information system enforces a limit of three consecutive invalid access attempts by a user during a/n [*organization-defined time period*] time period. The information system automatically *locks the account/node for 15 minutes*, when the maximum number of unsuccessful attempts is exceeded.	[redacted]	An assessment of a variety of components implementing this security control indicated that the implementation is not consistent system-wide and some components are not enforcing authentication policy as required by BEA policy. Two of [redacted] Windows components were not compliant with BEA policy (account lockout was not enabled).
AU-2 Auditable Events	The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].	[redacted]	Assessment of BEA policy found that it addressed the NIST SP 800-53 minimum requirements for this control. An assessment of selected system components revealed that audit and logging policy are not uniformly implemented throughout the information system. Four of [redacted] Windows components assessed were not compliant with BEA policy. One of the [redacted] devices assessed was not configured according to BEA policy requirements.
IA-2 User Identification and Authentication	The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	[redacted]	An assessment of a variety of components implementing this security control indicated that the implementation is not consistent system-wide and some components are not enforcing authentication policy as required by BEA policy. Two of [redacted] Windows components assessed did not have minimum password length set to 8 characters.

Table 5: Summary Comparison of Results from OIG Control Assessment and BEA Security Certification.

Control	Control Requirement	BEA's Security Assessment Report (SAR)	OIG Assessment Result (Summary)
IA-5 Authenticator Management	The organization manages information system authenticators by: (i) Defining initial authenticator content; (ii) Establishing administrative procedures for initial authenticator distr bution, for lost/compromised, or damaged authenticators, and for revoking authenticators. (iii) Changing default authenticators upon information system installation. (iv) Changing/refreshing authenticators periodically.	[redacted]	An assessment of a variety of components implementing this security control indicated that the implementation is not consistent system-wide and some components are not enforcing authentication policy as required by BEA policy. Two of [redacted] Windows components are not enforcing password history or minimum password age requirements. An additional Windows component had more stringent maximum password age settings (42 days) than BEA Windows Security standard—which raises a question about implementation of the standard across all devices.
SI-3 Malicious Code Protection	The information system implements malicious code protection.	[redacted]	Of the [redacted] components we examined, 12 had virus signatures that were out-of-date, with most being at least 60 days old.

Table 5: Summary Comparison of Results from OIG Control Assessment and BEA Security Certification.

<table>
<tr><th>Control</th><th>Control Requirement</th><th>BEA’s Security Assessment Report (SAR)</th><th>OIG Assessment Result (Summary)</th></tr>
<tr>
<td><b>CM-6</b>
Configuration Settings</td>
<td>The organization develops, documents, and maintains a current baseline configuration of the information system.</td>
<td>[redacted]</td>
<td>An assessment of a variety of components implementing this security control indicated that the implementation is not consistent system-wide.

[redacted] <b>components</b>:

Secure configuration baselines are well-documented for [redacted] components. Assessment of the running configurations revealed that some settings for logging were not in place for some network components—running [redacted] One [redacted] router and one [redacted] firewall had security settings that were not compliant with BEA-defined settings.

<b>Windows Components (Including [redacted]):</b>

Category I findings not addressed by or in conflict with BEA Windows Security Standards.

<table>
<tr><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td></tr>
</table>

In addition, our Gold Disk results revealed [redacted] unique Category II and 29 unique Category III findings exist on one or more of the 12 windows components assessed with the Gold Disk tool.

NOTE: The Category II & III findings are raw results and may have false positives counted in these figures.</td>
</tr>
</table>

Appendix A: Objectives, Scope, and Methodology

To meet the FY 2008 FISMA reporting requirements, we evaluated the BEA certification and accreditation for the Estimation Information Technology System (BEA-EITS, or BEA-015).

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** is based on the results of the security assessment. It documents actions taken or planned to address remaining vulnerabilities in the system.

Commerce'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.
- The **certification test results,** which is the raw data collected during the assessment.

To evaluate the C&A package, we reviewed all components of the package and interviewed BEA staff to clarify any apparent omissions or discrepancies in the documentation and gain further insight on the extent of the security assessment. We 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 security control assessments on BEA-EITS and compared our results with BEA's certification test results. We chose a subset of the control requirements specified in NIST SP 800-53, and a subset of assessment procedures from NIST SP 800-53A, Third Public Draft. We tailored the procedures to BEA's specific control implementations. We did not attempt to perform a complete assessment of each control; instead we chose to focus on specific aspects of some of the more important technical and operational controls.

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 BEA's certification test results while also targeting specific components that BEA did not test. We assessed control implementations on: [redacted] Windows components [redacted], [redacted]), and [redacted] devices [redacted]. In addition, we examined the security plan descriptions, including related policy documents, and interviewed appropriate BEA personnel.

Because of the importance of BEA's economic products, we adapted our assessments to minimize the impact on system operations. As a result, some assessments could not be performed on certain system components. For example, assessments involving the creation, modification, or deletion of user accounts on routers, firewalls, and switches were not performed. Our assessments included the following activities:

- Extraction, examination, and verification of system configurations
- Generation of system events and examination of system logs

- Execution of DISA scripts (Gold Disk)
- Examination of user and group authorizations
- Addition, modification, and deletion of operating system accounts

Our assessment was limited in scope and should not be interpreted as the comprehensive review that a security certification for a moderate impact system would require. However, our assessments gave us direct evidence of the status of select aspects of important controls in BEA-EITS and provided meaningful comparison to the BEA security certification.

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*
- NIST's 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*
    - 800-42, *Guideline on Network Security Testing*
    - 800-53, *Recommended Security Controls for Federal Information Systems*
    - 800-70, *Security Configuration Checklists Program for IT Products*

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

BEA
BUREAU OF ECONOMIC ANALYSIS
U.S. DEPARTMENT OF COMMERCE

U.S. Department of Commerce
Economics and Statistics Administration

August 12, 2008

MEMORANDUM TO: Judith J. Gordon
Assistant Inspector General for Audit and Evaluation
Office of Inspector General
Department of Commerce

FROM: J. Steven Landefeld JSL
Director

SUBJECT: Bureau of Economic Analysis
FY2008 FISMA Assessment of BEA Estimation
Information Technology System
Draft Inspection Report No. OSE-19001

Thank you for your recent draft assessment report of BEA's Certification and Accreditation package. In reference to your findings and recommendations:

Finding/Recommendation #1: The system security plan provided an adequate basis to conduct the security certification.

Response: We have worked hard on our comprehensive security plan, which forms the foundation of our security program, and would appreciate any suggestions that you may have for further enhancements.

Finding/Recommendation #2: BEA needs to improve its security control assessment to assure that controls are implemented as intended.

Response: The private sector contractors that we have used for the FISMA-required external assessments of our security controls have come to us with good recommendations. However, we would appreciate OIG's assistance in finding consultants who can be more successful in producing the more rigorous documentation that you detailed for these external assessments.

Finding/Recommendation #3: BEA needs to correct its process for tracking and reporting security weaknesses.

Response: BEA carefully tracks, tests, schedules, and implements all security requirements; however, as noted in the OIG report our process has not included provisions for assuring that this information is filed with, and made available to, the Department's OCIO through Plans of Actions and Milestones (POA&Ms).

Finding/Recommendation #4: Assessment of selected BEA security controls found weaknesses in those controls that BEA's certification did not.

Response: The Bureau continuously monitors the effectiveness of our security controls. Our first priority is the protection of critical market sensitive and company confidential data. As a result we had devoted the bulk of our scarce resources to protecting that core data.

However, we understand the importance of protecting the entire system, and are expanding the scope of our continuous monitoring program to ensure coverage of all system components.

Attached documents contain specific comments, and detail actions taken, in response to your report. BEA appreciates your recommendations and we are using them to further improve the Bureau's IT security program.

Attachments

cc: Rosemary Marcuss, Suzanne Hilding, Brian Callahan

BEA
BUREAU OF ECONOMIC ANALYSIS
U.S. DEPARTMENT OF COMMERCE

U.S. Department of Commerce
Economics and Statistics Administration

August 11, 2008

MEMORANDUM TO: J. Steven Landefeld
Director

FROM: Brian Callahan
Chief Information Officer

SUBJECT: Bureau of Economic Analysis
FY2008 FISMA Assessment of BEA Estimation Information Technology System
Draft Inspection Report No. OSE-19001

I reviewed the FISMA Assessment of the BEA Estimation Information Technology System. The recommendations in the report will serve to further strengthen BEA's IT security continuous monitoring program. The program is designed to mitigate new and ongoing threats to integrity and availability of the system.

BEA has addressed most of the points that were raised in the draft report. Specifically:

- We have increased the scope of our continuous monitoring program, with special emphasis on the NIST SP 800-53 technical control families. All tests, examinations, and interviews are performed by an independent contractor who reports directly to BEA's CIO. Test results are thoroughly documented with clear and appropriate artifacts. For each control family a Security Assessment Report is prepared for AO review and action. In addition the contractor performs random inspections of security defenses to ensure that they are performing as specified in BEA's Security Plan.

- Although not required [redacted] impact system, the Bureau had a team of independent contractors conduct a penetration test on BEA's information technology infrastructure. The team was unable to penetrate BEA's local area network but did provide some recommendations related to the external infrastructure which were promptly implemented.

- BEA continues to move forward in developing a standard configuration standard for Windows [redacted] servers. BEA utilizes the Defense Information Security Agency's (DISA) "Gold" as a secure configuration benchmarking tool. As the DISA documentation clearly states, each setting must be thoroughly tested before implementation in a production environment. BEA produces critical economic estimates such as Gross Domestic Product (GDP) monthly. BEA's risk-based secure implementation plan was designed with twin goals: benchmark and configure our most valuable assets first, and minimize the possibility of disruption in the ongoing statistical production process. Configurations for servers on BEA's Local Area Network which process our market sensitive and company confidential data were benchmarked and configured early in the process. We are now benchmarking less sensitive servers. This risk-based approach is reflected in the report where it is noted that some servers did not conform to our standard. In accordance with the report recommendation BEA has developed a Plan of Action and Milestones for completing this work across all servers.

- [redacted]

BEA is a small operating unit. To ensure the independence of the process BEA hires private sector firms to perform the certification of the BEA Information Technology Estimation System. Past successful performance has been the heavily weighted criterion in the vendor selection process. Unfortunately these vendors have not met the documentation expectations of the OIG. Our experience is that what is considered acceptable documentation varies greatly across agencies. BEA is determined to meet all applicable expectations and looks forward to working with the OIG and DOC CIO in developing written standards and a list of vendors whose work has met these standards. BEA has consistently volunteered to be an early implementer of the CSAM system. We believe that this system is a positive step in developing a standard approach to building system certification documentation packages.

BEA's IT staff benefited from the technical insights gained by working with the OIG reviewers. Hopefully we were able to provide the reviewers some insight as how the NIST InfoSec guidelines apply within a very operational/production-orientated technology environment.

Attached is a table that reflects the updated status of actions recommended in the draft report. BEA looks forward to discussing our continuous monitoring program with the OIG.

Attachment

Status of action items to address OIG recommendations

Synopsis of Finding	OIG Recommendation	Status of Action Item to Address Recommendation
1. System security plan provided an adequate basis to conduct the security certification.	1.1 Document secure configuration baselines with BEA's rationale for deviating from the benchmarks as appropriate.	[redacted]
	1.2 Update secure configuration baseline for [redacted] using the most current DISA benchmark available.	[redacted]
2. Security certification lacked credible supporting evidence for technical security control assessments.	2.1 Ensure all control assessments are supported by credible evidence to validate the assessment results.	[redacted]
	2.2 Ensure evidence shows that all applicable aspects of a control and an appropriate sample of components implementing it have been assessed.	
	2.3 Ensure assessment procedures and results include specific information about the implementation of the control and steps taken to assess it.	
3. Vulnerabilities	3.1 Comply with Department policy and	[redacted]

were not included in the security assessment report (SAR) or identified in POA&Ms.	guidance in tracking and correcting system security deficiencies.	[redacted]
	3.2 Create POA&Ms to address the Windows vulnerabilities described in the OIG report.	
	3.3 Explain vulnerabilities in SARs according to guidance found in NST SP 800-37.	[redacted]
	3.4 Articulate the vulnerabilities for which the bureau is accepting risk. Unimplemented secure configuration settings should be addressed in the SAR as well as the accreditation decision letter. If BEA chooses to redefine its secure baseline, that document should be updated with appropriate risk rationale.	[redacted]
4. OIG assessment of selected security controls found significant weaknesses not identified by the BEA security certification.	4.1 Ensure deficiencies the OIG identified are added to the system's POA&M and remediated in a timely manner.	[redacted]

		[redacted]
	4.2 Ensure control assessments are improved through tailored procedures and well-supported results which provide a transparent view of the status of controls.	[redacted].

Appendix C: Assessment of Selected Security Controls

A compact disk containing the procedures we used to assess security controls implemented on selected system components from the Estimation Information Technology System was provided to BEA. The disk also included our assessment results, analysis, and supporting evidence.

[redacted]