Withdrawn DOJ Privacy Impact Assessment

The attached Privacy Impact Assessment has been withdrawn and is provided solely for historical purposes. Information regarding this withdrawal appear, below.

Withdrawn Privacy Impact Assessment	
Title:	Certification & Accreditation (C&A) Web
DOJ Component:	Justice Management Division
Publication Date(s):	April 11, 2007
Withdrawn Date:	January 31, 2024
Withdrawal Note:	Following an updated review of this information system, JMD is not required to complete a PIA because the information relates only to internal government operations.

Superseding Privacy Impact Assessment *(if applicable)*	
Title:	
DOJ Component:	
Publication Date(s):	
URL:	
Supersession Note:	

Privacy Impact Assessment (PIA)

for the

Cyber Security Assessment and Management (CSAM)
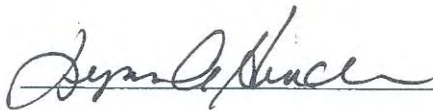
Certification & Accreditation

(C&A) Web (SBU)

Department of Justice

Information Technology Security Staff (ITSS)

April 11, 2007

Approval Signature Page

I recommend approval of the DOJ Information Technology Security Staff (ITSS)
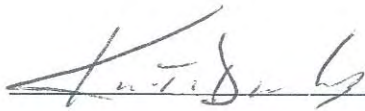Certification & Accreditation (C&A) Web (SBU) application Privacy Impact Assessment
(PIA).

(signature)   4-13-2007

Lynn A. Henderson   Date

System Owner, C&A Web (SBU) Application

Information Technology Security Staff

(signature)   4/27/07
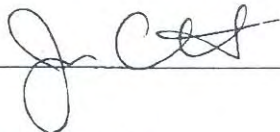
Kevin T. Deeley   Date

User Representative, C&A Web (SBU) Application

Information Technology Security Staff

(signature)   4-20-07

Jane Horvath   Date

Chief Privacy and Civil Liberties Officer

Department of Justice

Table of Contents

Introduction

C&A Web provides the DOJ IT Security Program, Program Officials and IT Security managers with a web-based secure network capability to assess, document, manage and report on the status of IT security risk assessments and implementation of Federal and DOJ mandated IT security control standards and policies.

FISMA emphasizes the need for each Federal agency to develop, document, and implement an enterprise-wide program to provide information security for the information and information systems that support the operations and assets of the agency including those provided or managed by another agency, contractor, or other sources.

The Department's IT Security Program has been elevated and strengthened over the past few years. The DOJ IT Security Program now takes a Department-wide view of its information security program. Fundamental in this initiative was the need to develop and implement a coordinated and effective IT security program that is continuous, interactive, and fully integrated within IT architecture and investment processes.

The C&A Web was collaboratively developed to be implemented within DOJ components as a streamlining initiative to achieve FISMA compliance and reporting requirements. C&A Web is a fundamental element of the DOJ IT Security Program enterprise architecture. It is an enterprise-wide tool for leveraging guidance from the National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), and industry best practices to assist the DOJ components in their IT security self-assessments and support management of FISMA reporting requirements.

C&A Web fully supports the implementation of the policy and procedures in Department's IT Security Program. The networked version of the required capability is required to support Department IT security program goals, system inventory and POA&M management process, FISMA reporting, required DOJ OCIO oversight responsibilities, and support of certification and accreditation and continuous monitoring process. With the C&A Web's functionality, system owners are allowed timely access to security information about their systems. The employment of a networked capability for this information posting and retrieval will facilitate access by Department managers.

C&A Web is critical to both C&A personnel and DOJ IT Security Program managers. C&A assessors will rely on the delivery of timely, detailed information and policy tool support related to IT Standards implementations. The use of the C&A Web application will enable system owners and security managers to obtain system performance information from a multitude of security related processes, while enabling the department and components to meet mandated enterprise and system reporting requirements.

C&A Web PIA Framework

The C&A Web PIA Framework provides programmatic information associated with the development and management of the C&A Web PIA.

Document Compliance
This C&A Web PIA complies with the Privacy Impact Assessment Official Guidance issues by the DOJ Privacy and Civil Liberties Office, effective August 7, 2006.

Document Organization
This C&A Web PIA applies the DOJ Privacy Impact Assessment Template (v3) (for a short-form PIA), as follows:

> Introduction
> Executive Overview
> Responses to questions, and summaries requested in Sections 1 through 6 and Section 8 of the afore-referenced template: (questions 1.1, 1.2, 2.1, 3.1, 4.1, 5.1, 6.2, 6.3, 8.9 apply)
> Conclusion
> Appendices

Document Audience
This document is intended for public access in accordance with OMB M-03-22 Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A/1.A.1.

Document Change Control
This C&A Web PIA is subject to the ITSS Configuration Control process as documented in the ITSS Configuration Management Plan.

C&A Web Contact Information
>   Name: C&A Web-SBU
>   Type System: Major Application
>   System Owner: Lynn Henderson
>   DOJ ITSS
>   202-616-0178
>   lynn.a.henderson@usdoj.gov
>
>   PIA Preparer: Ken Gandola
>   DOJ ITSS
>   202-353-0081
>   kenneth.d.gandola@usdoj.gov

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

The requirement to perform a Privacy Impact Assessment (PIA) for the C&A Web application was determined as a result of the Privacy Threshold Analysis (PTA) performed on the system. The PTA identified the requirement for a short-form PIA to be performed. Accordingly, the information follows for the following questions: 1.1, 1.2, 2.1, 3.1, 4.1, 5.1, 6.2, 6.3 and 8.9.

1.1   What information is to be collected?

C&A Web includes the Information in Identifiable Form (IIF) listed below, as defined in OMB Memorandum M-03-22/Attachment A/II.A.2.

- Name: Company; Government Staff; Contractor Staff

- Address: Company; Government Staff; Contractor Staff

- Telephone Number: Company; Government Staff; Contractor Staff

- Staff ID: Government Staff; Contractor Staff

- E-mail: Government Staff; Contractor Staff

1.2   From whom is the information collected?

Information is collected from parties to, or participating in IT Security system assessments and certification activities. Information is also collected from DOJ government and contractor IT security personnel who support the DOJ IT Security Program mission.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1　Why is the information being collected?

C&A Web fully supports the implementation of the policy and procedures in Department's IT Security Program. This networked application is required to support Department IT security program goals, system inventory and POA&M management process, FISMA reporting, required DOJ OCIO oversight responsibilities, and support of certification and accreditation and continuous monitoring process. With the C&A Web's functionality, system owners are allowed timely access to security information about their systems. The employment of a networked capability for this information posting and retrieval facilitates access by Department C&A testers, supervisors and managers.

To adequately document the status of meeting implementation of any security controls, evidentiary data is captured about the testing procedure. This typically involves the collection of information about tester interviewees that will have their name, phone number, position, title, email address and building location documented in the system.

2.2　What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

<< ADD Answer Here >>

2.3　Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

<< ADD Answer Here >>

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1　Describe all uses of the information.

The information that C&A Web application processes, stores and transmits is used to support the ITSS mission to implement the DOJ IT Security Program by ensuring the Confidentiality, Integrity and Availability of Information and Information Systems within DOJ.

C&A Web stores a body of historic information in SQL databases that are accessible to authorized DOJ users via the Intranet or through tools such as Business Objects.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

<< ADD Answer Here >>

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

<< ADD Answer Here >>

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

<< ADD Answer Here >>

3.5 <u>Privacy Impact Analysis</u>: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

<< ADD Answer Here >>

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

ITSS will share the C&A Web data, as appropriate, with the following internal components:

- Office of the Inspector General,

- All twenty-four DOJ components (utilizing three different versions of the application: one for SBU systems, one for classified systems, and one for the FBI). A separate PIA will be submitted for each of the three versions or systems.

4.2 For each recipient component or office, what information is shared and for what purpose?

<< ADD Answer Here >>

4.3 How is the information transmitted or disclosed?

<< ADD Answer Here >>

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

<< ADD Answer Here >>

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Information shared with external recipients is high-level statistics data, and not the actual raw data itself (such as the privacy data, such as names, phone numbers, etc.). Information is shared with the following external recipients:

- **<u>Office of Management and Budget (OMB) and Congress</u>:** OMB and Congress receive the following reports which include high-level statistical information based on information stored and processed by the C&A Web:

  - o Quarterly and annual reporting as required by Federal Information Security Management Act of 2002 (FISMA)

  - o Annual reporting as required by OMB Circular A-123, Management's Responsibility for Internal Control

- **<u>Contractor Operated Systems or Facilities</u>:** Contractor or contractor operated facilities that are involved with supporting DOJ systems that contains/processes DOJ data in personally identifiable form shall fall subject to the same technical, administrative and operational security controls as DOJ operated systems or facilities. Hence, applicable contractors are required to access C&A Web for documenting and reporting of IT security implementation status for relevant systems.

5.2   What information is shared and for what purpose?

<< ADD Answer Here >>

5.3   How is the information transmitted or disclosed?

<< ADD Answer Here >>

5.4   Are there any agreements concerning the security and privacy of the data once it is shared?

<< ADD Answer Here >>

5.5   What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

<< ADD Answer Here >>

5.6 Are there any provisions in place for auditing the recipients' use of the information?

<< ADD Answer Here >>

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

<< ADD Answer Here >>

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

<< ADD Answer Here >>

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Generally, individuals do not have the right to decline to provide information. The information gathered about individuals is required for two related but slightly different purposes, depending on the role in which the individual is acting:

FOR C&A Web SYSTEM USERS:

- As part of the standard procedures for requesting an account on the C&A Web system, a federal employee or contractor working for the DOJ must provide certain personal information to enable other users and administrators of the system to contact them as necessary. Email addresses are also required to enable to system to send automatic alerts to users.

- Any DOJ intranet or C&A Web user has already become familiar with and understands the Department of Justice (DOJ) Computer System User Information Technology (IT) Security General Rules of Behavior. DOJ Intranet users have agreed to the General Rules of Behavior, along with being familiar with and understanding them.
  - o The current version is Version 2.0 dated May 23, 2005.
  - o These rules extend to all DOJ personnel (employees and contractors) and any other persons using DOJ computing resources or accessing DOJ systems under formally established agreements.
  - o All users should be fully aware of, and abide by, DOJ security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and DOJ Records Management Regulations.

FOR Personnel with IT Security responsibilities (government employees, government contractors at government facilities or contractor operated facilities):

- Any individual that is involved in any IT Security responsibilities relating to a DOJ information system is subject to having privacy information about them captured and recorded in the C&A Web database. The individuals may not be aware that the information was captured in this fashion. Typically, anyone performing in an IT Security responsible position is subject to being interviewed during the system assessment procedure. To adequately document the status of meeting implementation of any security controls, evidentiary data is captured about the testing procedure. This could typically involve the collection of information about the tester interviewees that will have their name, phone number, position, title, email address and building location documented in the system. If these individuals declined to provide their name, phone number, position, title, email address, and building location, it would seriously impact the DOJ's ability to perform its responsibilities for continuous monitoring of security controls and oversight of the Department's IT Security Program.

6.3 **Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?**

For those individuals (as described above), there is no consent to the specific uses of the information captured or maintained in the C&A Web system. The Rules of Behavior that all system users have signed identified the conditions under which access to a DOJ Information system impacts their privacy information and the requirements to properly handle/use and access to privacy information.

6.4 **Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.**

<< ADD Answer Here >>

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 **What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?**

<< ADD Answer Here >>

7.2 **How are individuals notified of the procedures for seeking access to or amendment of their information?**

<< ADD Answer Here >>

7.3 **If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?**

<< ADD Answer Here >>

7.4 **<u>Privacy Impact Analysis</u>: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.**

<< ADD Answer Here >>

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 **Which user group(s) will have access to the system?**

<< ADD Answer Here >>

8.2 **Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.**

<< ADD Answer Here >>

8.3 **Does the system use "roles" to assign privileges to users of the system?**

<< ADD Answer Here >>

8.4 **What procedures are in place to determine which users may access the system and are they documented?**

<< ADD Answer Here >>

8.5 **How are the actual assignments of roles and rules verified according to established security and auditing procedures?**

<< ADD Answer Here >>

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

<< ADD Answer Here >>

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

<< ADD Answer Here >>

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

<< ADD Answer Here >>

8.9 <u>Privacy Impact Analysis</u>: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

<u>Threat</u>: Unauthorized Access to the C&A Web system
<u>Risk</u>:   Low
<u>Mitigation/Countermeasures</u>:
- **<u>Security controls</u>**. The C&A Web is a web-based system hosted within the Justice Data Center- Washington in a fully Certified and Accredited (C&A) DOJ intranet production environment according to generally accepted DOJ standards and guidelines for C&A of systems and networks for the department.
    - A total of 74 security controls are applicable for the C&A Web system.
    - A total of 69 security controls are inherited for the system.
    - Twenty security controls are not applicable according to the system categorization and scoping of the C&A Web Requirements Traceability Matrix (RTM).
    - **<u>Authentication/Access controls</u>**.
        - A total of 10 AC family security controls are applicable for the C&A Web system.
        - A total of 10 other AC family security controls are inherited by the C&A Web system from the GSS production environment.
        - Any C&A Web or intranet user is required to be familiar with the DOJ General Rules of Behavior for information system use.
        - Initial access to the C&A Web online system is limited to authorized users with active C&A Web accounts on various closed Sensitive But

Unclassified (SBU) local area networks (LAN) amongst the various DOJ components. Multi-layered security is in effect by virtue of the fact that users must first logon to JCON (or other DOJ desktop/intra-networks) and then access the C&A Web after a successful LAN authentication. An unauthorized user would be need to have knowledge of both userID/password combinations in order to gain access to the C&A Web.

- o **Role-based access controls**. Access to specific data is restricted by user classification (as assigned by roles and privileges).
  - This procedure enforces access control to information with privacy implication to members of an assigned role as determined appropriate by the user's supervisor and profiled accordingly in the C&A Web system by the system administrator(s).
  - Roles and privileges can be assigned at the component, system, control and user levels.
  - Each user is profiled by approval authorities that then notify the C&A Web system administrator of the appropriate roles and privileges authorized for each individual (user) for proper security settings in the account management function of the C&A Web.
  - C&A User accounts can be created, updated, enabled and disabled only by authorized system administrators, upon receiving input from authorized approval authorities. To perform these functions, the system administrator(s) must be identified and profiled for such privileges in the C&A Web.
  - System Administrators will:
    - Ensure that the certification agent or CA-appointed agent validates system security at least annually.
    - Make the computer(s) available for periodic reviews of the security configuration by independent testers.
    - Ensure that under no circumstances the same person serves as the system administrator and ISSO for the same system.
  - Managers will:
    - Ensure that staff has access to, and sufficient time to complete, the DOJ Computer Security Awareness Training (CSAT), or other annual IT security training offered by offices/bureaus/components not utilizing CSAT.
    - Ensure that staff has access to, and are aware of, all existing DOJ policies and procedures (DOJ Order 2640.2(series), DOJ IT Security Standards) relevant to the use of DOJ information technology resources.
    - Ensure that staff follows system security policies, guidelines and procedures (DOJ Order 2640.2(series), DOJ IT Security Standards).

- o **Audit controls.**
  - ▪ A total of 6 AU family security controls are applicable for the C&A Web system.
  - ▪ C&A Web data input/changes can be tracked through database logging and auditing functions. Auditing logs are designed to be checked on a routine basis and monitored by system administrators. Access and changes to C&A Web data is captured in audit logs that are assigned to privileged individuals with appropriate system roles to monitor the audit logs.

Threat: Remote Access to the C&A Web system data
Risk: Low
Mitigation/Countermeasures:
- Selectively authorized and established remote access accounts for any remote C&A Web system access follow established DOJ policies and procedures for issuance of individual JSRA accounts. Remote access is only permitted with valid authorization by supervisors and issuance of a JSRA account authorizing remote access privileges.
- Remote users are informed that they too must have a responsibility to take measures to protect the C&A Web system data they access from their remote site. Remote users must do everything they can to protect data from being compromised or captured on their computers, especially when using personal computers at home. These precautions may include:
  - o Installation of operating system and application software (i.e. Internet Explorer) updates regularly. Many of these updates are issued to fix security problems which have been identified.
  - o Install and use anti-virus software and personal firewalls and keep this software updated.
  - o Do not store your various User-IDs and passwords in files on your computer.
  - o After using your browser (e.g. Internet Explorer, etc.) to access a site where you process sensitive information close all of your browser windows and restart a new browser session. Sometimes the browser can hold that information in memory (e.g. cache, etc.) and some websites know where to look to find it.
  - o Be very careful when installing software that gives others access to your computer. Remote service software or peer-to-peer software used for file sharing can create unintended openings into your computer that outsider can use if the software is not configured correctly.

Threat: Unauthorized Disclosure of the C&A Web system data
Risk: Low
Mitigation/Countermeasures:

- Reports can only be printed by authorized users and authorized users have accepted rules of behavior, which includes the proper handling of sensitive system security paperwork for SBU system data, whether it is a physical printout or access to the system.

Section 9.0
Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1   Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

<< ADD Answer Here >>

9.2   Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

<< ADD Answer Here >>

9.3   What design choices were made to enhance privacy?

<< ADD Answer Here >>

Conclusion

The C&A Web application is used to process, store, and transmit information that supports the DOJ IT Security program. Securing this information and assuring its proper use is critical to the success of this DOJ and ITSS mission and related operations.

The C&A Web is secured via access authorization, authentication rules, and audit controls. These technical controls are supplemented by procedural controls such as Account Management Reviews, Rules of Behavior, Confidentiality Agreements, and Security Awareness and Training to mitigate risks regarding unauthorized access and subsequent potential privacy

violations. The proposed Defense-in-Depth implementation will increase the robustness of C&A Web security services, i.e., access controls, confidentiality, integrity, and non-repudiation.

ITSS has consistently regarded the privacy ramifications of information that is processed, stored, and transmitted in the C&A Web application as critical in supporting the DOJ IT Security Program. The C&A Web solution is aligned with supporting all of DOJ's security objectives via application of FISMA requirements and industry Best Practices. Management review, continual enhancement, and FISMA-mandated continuous monitoring of C&A Web technical and procedural controls are of the utmost importance in maintaining application hardening and continuity of operations.

<u>Appendix A</u>: References

E-Government Act of 2002, Public Law 107-347, Section 208(b)
Freedom of Information Act (FOIA) (as amended), 5 U.S.C. 552
Privacy Act (PA) of 1974 (as amended), 5 U.S.C. 552a
OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources

OMB Memorandum M-06-20 FY 2006 Reporting Instructions for the **Federal Information Security Management Act and Agency Privacy Management** (17 Jul 2006)
OMB Memorandum M-06-16 Protection of Sensitive Agency Information (23 June 2006)
OMB Memorandum M-06-15 Safeguarding Personally Identifiable Information (22 May 2006)

FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

NIST SP 800-53 Recommended Security Controls for Federal Information Systems
NIST SP 800-37 Guide to the Security Certification and Accreditation of Federal Information Systems
NIST SP 800-30 Risk Management Guide for Information Technology Systems
NIST SP 800-18 Rev 1 Guide to System Security Plans for Federal Information Systems

DOJ Order 3011.1A Compliance with the Privacy Requirements of the Privacy Act, The E-Government Act, and the FISMA
DOJ Privacy Impact Assessment Official Guidance Manual August 7, 2006
DOJ Memorandum issued on 10-July-2006, Privacy and Safeguarding of Personally Identifiable Information

Appendix B: Abbreviations and Acronyms

CSAM	Cyber Security Assessment and Management
C&A	Certification & Accreditation
DBA	Database Administrator
DOJ	Department of Justice
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
GSS	General Support System
ITSS	Information Technology Security Staff
JMD	Justice Management Division
MA	Major Application
MIS	Management Information Systems
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
SBU	Sensitive But Unclassified
SC	Security Category
SDLC	System Development Life Cycle
SORN	System of Records Notification
SP	Special Publication
SSP	System Security Plan
UPI	Unique Project Identifier