Criminal Investigation – 2 General Support System (CI–2 GSS) – Privacy Impact Assessment

PIA Approval Date – Jul. 20, 2011

System Overview

The Criminal Investigation2 General Support System (CI–2 GSS) provides Criminal Investigation (CI) Case Agents, CI Analysts, CI Computer Investigative Specialists (CIS) and CI Special Agents a means to collaborate on CI cases and efficiently analyze case evidentiary data. The goal is to effectively preserve, store, analyze, and process seized data in a forensically sound manner to support criminal investigations. The CI–2 GSS provides users with the necessary infrastructure to securely access and collaborate on seized evidentiary case data. The entire solution of CI–2 GSS ECE added functionality, revolves around the ability to centrally manage and execute forensic tools to analyze, bookmark, and process seized forensic data in order to provide evidence for an electronic crimes–related case in court. The forensic analysis environment tools will receive evidence (forensic images of a system or systems) uploaded to the ECE evidence repository within the CI–2 GSS. The process is manual and required in order to move to the next phase of processing. The environment in which the physical evidence seized, by the CIS is imaged, which is normally done remotely by a local CIS imaging tool, also encrypting the evidence. After the capture of the image, the CIS sends it to the CI–2 GSS Evidence Custodian. The Evidence Custodian receives it and validates the hash value to ensure that the original physical evidence was not tampered or altered. After decrypting the image, the validated image file is then uploaded by the CI–2 GSS Evidence Custodian, which is then ready (evidence image) for forensic processing by the CIS.

Systems of Records Number(s) (SORN) #:

- IRS 46.002--Criminal Investigation Management System
- IRS 46.009--Centralized Evaluation and Processing of Information, Criminal Investigation Division
- IRS 46.022--Treasury Enforcement Communications Systems, Criminal Investigation Division
- IRS 46.050--Automated Information Analysis System
- IRS 34.037--IRS Audit Trail and Security Records Systems

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer – The GSS may contain sensitive information in the form of work products to include the following types: Taxpayer information depending on the evidentiary case information seized contained in the evidence containers, contained within the CI–2 GSS. Evidentiary case data in supporting Priority #1 (E–1) and Priority #3 (CBP–11) IRS Critical Business Processes, including both administrative and grand jury case information relating to title 26, tax related violations, money laundering, narcotics and counter terrorism. All items of Personally Identifiable Information (PII) could be available in employee work product or evidentiary case data.

B. Employee – The GSS may contain employee user information for the purposes of authentication. Potential elements of employee information are:
   - Employee name
   - Employer user identifier

C. Audit Trail Information – Current lists of authorized users and their access authorizations are maintained on each CI–2 GSS component capable of recording such information. A matrix of user rights has been created and maintained by the Evidence Custodian to disallow unauthorized data viewing and manipulation. This information (excel spreadsheet) would be added to the case file. This information can be available upon request for those who have a legitimate need to know in accordance with IRS IRM 10.8.1.5.2 (7).

CI–2 uses audit records to review what occurred after an event, for periodic reviews, and for real–time analysis. Audit records allow management to hold employees accountable for their actions within the CI–2 GSS. Only the authorized system and security administrators are assigned the responsibility to review audit information.

CI–2 system administrators are responsible for reviewing performance logs for all CI–2 GSS components; and the CI–2 security administrator is responsible for reviewing system logs for all CI–2 GSS components. Audit log review is done manually on a regular basis.

The security administrator is responsible for reviewing system audit logs for suspicious or unusual user activity and/or behavior. The security administrator will first review and request the entire audit trail. In some cases, the event might trace all the way back to the CI–1 GSS and/or user's workstation. In this case, the security administrator would contact the appropriate CI–1 security personnel for support in investigating this behavior.

Due to the sensitivity of the CI–2 environment, anything unusual that warrants investigation is immediately reported to local Electronic Crimes upper management by either the security (for system events) or system administrator (for performance events). At this point, upper management can authorize additional investigation and review if warranted. If deemed necessary, upper management and/or administrators would report the concern to the C–1 Help Desk.

CI–2 system administrators increase the level of audit monitoring, review, and analysis whenever there is an increased risk to organizational operations, assets, or individuals. System administrators are constantly in tune with any threats or risks identified by law enforcement organizations, the intelligence community, and/or other credible sources.

Event/system logs generated and stored within both the virtual RedHat and Microsoft servers are not regularly reviewed on a weekly basis by the security administrator. Due to the sensitivity of data stored within the virtual case data servers, event audit logs are stored directly in the corresponding containers themselves. As part of trial preparation, audit logs are reviewed in full by the case agent assigned the case. Due to the sensitivity of this information, the event audit logs cannot be released to CI–2 administrators unless unusual or inappropriate behavior is suspected and the release of information is approved by upper management.

The CI–2 GSS has a total of nine main categories of users (4 prior designated roles and 5 additional ones):

- System Administrators
- Security Administrators
- Evidence Custodians
- CI–2 CIS/Investigators
- User/Special Agent

- Supervisor
- DBAdmin
- Developer
- Monitor

Auditable events are documented in Law Enforcement Manual (LEM) 10.8.3. The IRM states that all IRS information systems, applications, and databases capture and record the auditable events based on their FIPS 199 overall system security categorization. Every interaction with Taxpayer Data through the CI–2 GSS is an auditable event and shall be audited. Also, the IRM states that for each event, an automated response is required. CI–2 System Administrators and Security Administrators each have established responsibilities for maintaining the configuration of CI–2 technology devices and software, and enable and configure audit logging on all IRS systems in accordance with LEM 10.8.3 and IRM 10.8.2.

CI–2 GSS components are capable of compiling all audit records within each device into a system wide, time–correlated audit trail. Additionally, each component provides the capability to manage the selection of events to be audited utilizing built in system firmware and management software.

Periodic reviews are conducted to update the list of organization–defined auditable events. The list of required audit events is detailed in LEM 10.8.3, Audit Logging Security Standards which is maintained by MITS Cybersecurity, is periodically reviewed, and updated if necessary by MITS Cybersecurity.

Previous partial Risk Based Decision, found on Table 13 of the CI–2 GSS Security Assessment Report, dated December 18th, 2010, R–RBD–14, will be mitigated with the funding obtained via the ECE Project, replacing both the current 3com and Foundry legacy switches. Current CI–2 GSS PO&AM R–16–2011–AC11_12.1 mitigation strategy mentions replacement of legacy hardware, since during prior recertification, for the AU–2 Security Control, CI–2 GSS had a partial RBD. During this year’s monitoring cycle, the CI–2 GSS SSP and appendices will be updated prior to the ECE enhancement project receiving its MS4b exit approval.

ECE functionality auditable events can be found on the approved ECE PIA, dated May 16, 2011.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. Employee data elements – The employee inputs work products into CI–2 GSS, evidence container, assigned to them; however this work product could contain employee's User ID or Name, but does not contain any other Personally Identifiable Information about the employee.

B. Other Fed agencies data elements – Dependent upon the case, CI–2 GSS can receive data in the form of evidence or work products that is only available to the CI–2 GSS user, to their respective evidence container from the employees of another federal agency. Federal Bureau of Investigation, Secret Service, Immigration and Customs Enforcement, Postal, or any other federal agency could provide data in the form of work product. The work product could be case images, records, data sets, or other electronic data related to a criminal investigation.

C. State and Local agencies data elements – Dependent upon the case, CI–2 GSS can receive data in the form of evidence or work products from the employees of state and local agencies.

D. Other 3rd party data elements – Dependent upon the case, CI–2 GSS can receive data in the form of evidence or work products from other third party sources.

3. Is each data item required for the business purpose of the system? Explain.
Yes. All information contained on the system is present on a case–by–case basis and supports the enforcement and investigative purpose of the system.

4. How will each data item be verified for accuracy, timeliness, and completeness?
CI–2 GSS incoming data is validated for accuracy and completeness by using hashing algorithms and time stamps. When timeliness is an issue for CI–2 GSS user, the date time stamp is used to verify the time the data was created, as verified during recent recertification for SI–10 Security Control. Data is created from investigative research and CI–2 GSS receives duplicate data from law enforcement agents. The agent (CIS/CI–2 GSS user) is responsible for ensuring that the data is accurate and complete

5. Is there another source for the data? Explain how that source is or is not used.
In most instances, any third party data would be obtained by the Agent; however, there may be instances where another source provides third party data depending on the case. Investigative purposes require that these data elements be collected to support the investigation regardless of whether or not another source exists. Evidentiary data is always delivered to us in the form of a copy of the original from the Agent (CIS/CI–2 GSS User). CI–2 GSS does not hold the original evidentiary data from a case. There is always at least one other copy of it, besides the original data, that is not stored within CI–2 GSS. Data is in the form of work product. Data could be research documents that Agents (CIS/CI–2 GSS user) create or it could be case information which could be in the form of a forensic image or data set using the tools within CI–2 GSS, via the ECE evidentiary container.

6. Generally, how will data be retrieved by the user?
The authorized OL5081, CI–2 GSS Agents (CIS/CI–2 GSS user) will be retrieving copies (i.e. screen shots) of file level data they are authorized to access using operating CI–2 GSS System level, built–in functions (i.e. a https secure connection established to virtual resources via a secure application proxied connection through the CI2 Cisco ASA gateway) or forensic search tools, within their assigned evidence container. Outputs such as reports are printed manually, as needed, as elaborated below. Approved copies of actual files, may be transferred and downloaded thru secured Cisco Security Gateway portal access – scanned and placed in a file within CI–2; that would allow access to CI–1 for the approved Agent to retrieve.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data on the system can be retrieved by a unique identifier, but is only accessed using forensic tools in support of a case investigation. Those forensic tools can only be used within the assigned evidence container on files pertaining to that case and only within the scope of that investigation. Computer forensics software (tools) use a variety of electronic processes and specialized techniques for recovery, authentication, and analysis of electronic data in raw bit form when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage.

Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end–users or system support personnel. CI–2 GSS evidentiary

case data, residing on the respective evidentiary case container, residing on CI–2 GSS system that is network attached is stored in a proprietary format which is encrypted and not searchable unless by authorized user with the use our CI–2 GSS proprietary software tool.

This data is further protected by NTFS permissions in which read access is granted to only the individuals that have a need and authorization to see it, per their respective user role identified via the EA OL5081 process, in conjunction through Criminal Investigation's internal ECMIS tool, after appropriate CI CCB and TAB boards approve the initial OL5081 to enforce physical and logical access restrictions associated with the Agents (CIS/CI–2 GSS user) designated access, enforcing least privilege.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

CI–2 GSS is not accessible and/or available to the general public. The CI–2 GSS Roles are listed below:

Role: System Administrators
Permission: System administrators perform all administrative functions and are the only people authorized to make changes to this GSS (i.e. The system's hardware and architectural components such as network configuration, storage configuration, and virtual environments are modified, maintained, and controlled by this set of staff. This role also has the ability to allow for export of non encrypted files that are a part of a designated approved resource). They maintain a list of approved users and their respective permissions in order to disallow unauthorized data viewing for manipulation.

Role: Security Administrators.
Permission: Security administrators do not make any changes to the CI–2 GSS, though they review audit records and have Cyber access to logs reflecting all such changes to the information system and monitor the changes that are made by the system administrator. The security administrators will also review all audit changes to reflect all such changes to the system, and ensure the security of the system is maintained.

Role: Evidence Custodians
Permission: Evidence custodians have write and read access permissions within the virtual containers they maintain. Write permissions are only required for uploading delivered evidence into each virtual evidence container in the Electronic Crimes Environment (ECE). The evidence files themselves are read only for both regular end users and Evidence Custodians. Once seized, this information cannot be altered; the integrity of the data is validated by the hash value and then the custodian properly provisions the individual CIS' evidence analysis environment. Evidence files are hashed to ensure data is never altered once in the system.

Role: CI–2 CIS/Investigators
Permission: CI–2 CIS/Investigators cannot make any changes to the system, nor have access logs or development tools; however, their assigned evidentiary resource pool of which they have administrative rights through 3rd party management apps, which do not allow system access. They have approved assigned responsibility for managing evidence processing analysis, and access by Case Agents (CI–2 "User"), once authenticated via the CI–2 GSS ASA gateway. They also have administrative rights to VMs created in their resource pool, as well as, have the ability to create, and destroy VMs in resource pool. They also have the ability to add software to VMs in resource pool.

Role: User/Special Agent (SA),
Permission: User/Special Agent (SA) are the lowest level special agents has the ability to work and receive access to his/her workspace from the CI–2 GSS CIS created evidentiary Virtual Machines to analyze the evidence, prepare his/her presentation, and create reports using analytical tools. This role has the ability to export all or some of the required data through CI–2 GSS Electronic Crimes Environment (ECE) approved defined processes. This role does not have admin rights to the VM.

Role: CI–2 GSS Supervisor
Permission: CI–2 GSS Supervisor has the ability to interact with all evidentiary systems as a local administrator. He/she has the ability to restore files and snapshots. They also ensure that evidence housed within the evidence containers, in the Electronic Crime Environment (ECE), and are properly allocated to specific cases, CIS', and Special Agents. He/she also manages the creation and provisioning of virtual machines based on special cases. This role is also a subject matter expert on the forensic tools and governs its use on the CI–2 GSS, within electronic crimes environment. This role also has the ability to allow for export of non encrypted files.

Role: CI–2 GSS DBAdmin
Permission: CI–2 GSS DBAdmin role maintains the CI–2 GSS Electronic Crimes Environment (ECE) database (a sub–component of CI–2 GSS), which is updated from ECMIS. NOTE: ECMIS is a separate system, within eCrimes Lab that compliments the OL5081 process and is exclusively used within CI.

Role: CI–2 GSS Developer
Permission: CI–2 GSS developer role was created, for preparation of connecting ECE Test/prod to CI–2 GSS in June, for future SCA testing in the production environment (similar to the IDA application, which now resides on the CI–1 GSS). We needed a role for the BAH developers whom are cleared.

Role: CI–2 GSS Monitor
Permission: CI–2 GSS monitor role was created to monitor activities in the ECE crimes database, associated engineering and development actions and receive and review alerts and system notifications.

Note: The eCrimes Forensic Tools are for CI Internal use only. They are only available to locked–down virtual systems which are configured with non–routable networking in the CI–2 GSS by trained CI/CIS Agents. The Forensic Tools cannot be accessed from IRS or CI networks. There is no impact to other areas than limited resource groups in the CI–2 GSS.

9. How is access to the data by a user determined and by whom?
Access to the data by a user is determined, by a combination of an EA enterprise automated system, via the EA OL5081 process, in conjunction through Criminal Investigation's internal ECMIS tool, after appropriate CI CCB and TAB boards approve the initial OL5081 to enforce physical and logical access restrictions associated with the Agents (CIS/CI–2 GSS user) designated access, enforcing least privilege using the CI–2 GSS authentication via CI–2 GSSs active directory. Additional information can be found in the current CI–2 GSS, main SSP, version 2.0, dated December 18th, 2010, under the AC–2 Account Management security control, as well as, the specified user role description above.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
No.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Not applicable. However, the ECE Project, which is part of the existing CI–2 GSS, did submit a separate PIA. It was approved on May 16th, 2011. Information contained in the ECE PIA has been included in this updated CI–2 GSS PIA.

12. Will other agencies provide, receive, or share data in any form with this system?
Yes. Data is received from other federal, state and local agencies as well as third parties as needed on a case–by–case basis to support an investigative need. CI–2 GSS does not share taxpayer–related data/information with any agency. However, Agents/users/CISs, can assist other agencies with data relating to an investigative need depending on the nature of the crime and the jurisdiction of the supported agency. Lastly, CI–2 GSS receives data from other agencies.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
After CI's consultation with Criminal Tax Counsel and the Department of Justice, CI is following the recommendation per the signed Memo, September 21, 2010 by Victor Song, initiated on September 17, 2010, for data residing on the CI–2 GSS.

CI follows IRM 1.15.43, in providing that electronic copies of records other than the "recordkeeping copy", be destroyed or deleted within 180 days after the record keeping copy has been produced. The exception is regarding litigation holds; CI adopts a 180–day retention policy for monthly backup tapes. This retention policy would be in keeping with that of IRS–MITS and would resolve the growing logistical difficulties of storing the monthly backup tapes indefinitely. Moreover, because the case–related material contained on the backup tapes duplicates material that is maintained elsewhere, destruction of the tapes would not compromise our ability to comply with criminal litigation discovery requests. Following the expiration of the 180–day period, the tapes would be recycled or destroyed, in keeping with existing media destruction policy.

The only exception to the proposed 180–day retention period for monthly backup tapes would be for situations where there is an existing litigation hold imposed by the Department of Justice, the Office of Chief Counsel, or a specific court order. The 180–day period would be suspended for backup tapes under the purview of a litigation hold. The Technology Operations & Investigative Services E–Discovery Program (EDP) would be responsible for monitoring litigation holds and for notifying appropriate TOC personnel when the suspension could be lifted. Prior to recycling or destroying any tapes, the local custodian would review EDP Sharepoint for any applicable litigation hold.

The Lead Agent (CIS/Investigator) will dispose of the records in accordance to ITM 15.15.30–1(15) for Criminal Records Retention. Copies of the audit logs are moved to long–term storage and are maintained as per IRM 10.8.3

14. Will this system use technology in a new way?
Yes, in implementing the GPRA Modernization Act of 2010, the CI eCrimes goal for the CI–2 GSS, is to look for Operational Improvements. The operational improvements identified, during our prior recertification, are being addressed by upgrading our hardware (which also mitigates previous vulnerabilities); and purchasing new forensic software tools that will be centrally located on our CI–2

GSS, we are reducing cost in providing forensic analysis/investigations in a more efficient method, as well as; eliminate future additional costs, by not having to upgrade current Agents stand–alone computers with new forensic technologies. The CI Electronic Crimes, CI–2 GSS is leveraging emerging new forensic technologies to ensure that digital evidence is used efficiently and to the greatest extent possible in this current climate of our expanding electronic economy, thus achieving improved, cost effective, and decrease investigative timeframes. In doing so, we are continuing to support supports the E–1 and CBP–11 IRS Critical Business Processes.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No; however, thru the forensics analysis/ investigative process, supported by the CI–2 GSS, the user could potentially locate or identify individuals or groups, as part of their investigation.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No; however, thru the forensics analysis/ investigative process, supported by the CI–2 GSS, the user could potentially locate or identify individuals or groups, as part of their investigation

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No; however thru the forensics investigation process, within the assigned evidence container, within the CI–2 GSS, the information could treat taxpayers, employees or others differently as a matter of an investigation or criminal prosecution.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not Applicable. The CI–2 GSS does not make any negative determinations; the recommendation to prosecute comes from the case Agent/CIS/user.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No. The CI–2 GSS is not web–based.

View other PIAs on IRS.gov