Privacy Impact Assessment
for the

Remedy System

November 15, 2006

Contact Point
Luis Vega, 202-648-9411

Chief, Operations Performance Management Section
Information Services Division (ISD)

Office of Science and Technology
Alcohol, Tobacco, Firearms and Explosives (ATF)

Reviewing Official
Jane C. Horvath
Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 514-0049

Introduction

The Remedy System is a Commercial off the Shelf application that incorporates help desk trouble ticket functionality, change management functionality, Service Level Agreement (SLA) and asset management functionality. The Remedy System also incorporates an e-mail engine and an approval engine. The system's major purposes are to provide for an integrated approach to Information Technology (IT) help desk service management. The system automates support processes including the ability to submit, monitor, and manage IT help desk cases, change requests and asset inventory records. Most recently the system has been modified to include an automated application request system and also a tracking system for field agents, Intelligence Division personnel, and ATF Headquarters personnel. Remedy resides in a Raleigh helpdesk facility. The system has a hot backup that is housed in the ATF Cherokee Data Center.

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.

1.1 What information is to be collected?

Information important to the resolution of IT issues is created in the form of a ticket. In some cases this is a trouble ticket, in some cases this is a change (access control) ticket that might need approval and in other cases this is an asset ticket where a piece of equipment might need to be replaced or purchased. In order to identify users who contact the help desk the caller's information is held in Remedy Persons Information Form. This data includes the division, site and address, phone number, organizational code, last four of social security number (SSN), date of birth, mother's maiden name, first name, last name, the type of employee they are, the agency they belong to, the employee identification number, who their manager is, are they a manager and what level of service they will receive. This information is used to confirm the identity of the caller and to determine where he/she is located. The employee identification number is not the user's SSN; it is a set of numbers generated by HR Connect, an ATF Human Resources system. The employee identification number is used as a unique key to import HR Connect data into the user's Remedy profile. The last 4 digits of the Social Security Number is the standard way a user is identified when placing a call to the Help Desk. External users require two forms of verification: date of birth (DOB) or mother's maiden name. There is no validation to DOB or mother's maiden name so once a user is properly identified they may provide a fictitious date or fictitious name. The technician will create the ticket as long as the information that the user provides matches the information in Remedy Persons Information Form. For several applications in E-Request a complete SSN

is required (N-force, N-Focus, N-Quire and N-spect). When the full SSN is asked for, the requester must put in the full SSN, which is immediately encrypted. Only the system owner can see the full SSN. It has been recommended that we go to a secret question type of scenario, where for example, we ask the user's home town or elementary school. Information about the technician working on the caller's request is captured in the worklog, to include the technician's login. No other information is captured about the technician in the ticket. If a Drivers license number and state are captured in RFI it is encrypted. If a License plate number along with state is captured, it also is encrypted. Sex, Race, DOB age, nick names, alias', alternate social security numbers, alternate DOBs are also captured, but are not encrypted.

1.2 From whom is the information collected?

The information is collected mainly from ATF government and contractor support personnel. There are three exceptions with the collection of information for help desk support: the Bomb Arson Tracking System (BATS), the Electronic Trace Submission System (E-Trace) Application, and the Firearms and Explosives Imports System FIT Imports Web (eForm6). BATS is used by the local fire and police agencies to streamline the gathering, retrieving, reporting, and archiving of incident investigation information contribution by valid law enforcement agencies engaged in the investigation of fire, arson, bombings, and the criminal misuse of explosives. E-Trace is used by ATF, various law enforcement agencies and police departments to submit firearm traces to the ATF National Tracing Center (NTC) via the internet. eForm6 is an application for the importation of firearms, ammunition, explosives and implements of war. In all these cases, Remedy is used by the Help Desk to reset passwords and to assist with application level problems only.

The caller's information held in Remedy Persons Information Form, includes the division, site and address, phone number, organizational code, last four of SSN, date of birth, mother's maiden name, first name, last name, the type of employee they are, the agency they belong to, the employee ID number, who their manager is, and if a manager what level of service they will receive. Since these applications all contain sensitive law enforcement data, this information is used to confirm the identity of the caller and then know to where he/she is located. The rest of the ticket information is captured to know the type of problem the caller is having and reason for the call.

The Remedy Team has not been allowed to have a constant feed from HR Connect, so no other capability exists to get the authentication data, other than to store it in Remedy. Justice sends data to ATF, and the ATF Human Resources Division currently sends a spreadsheet to the Remedy Development Team twice a week.

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?

The information specific to the person is critical to identifying the person especially when there is a request to reset a password. The information collected regarding equipment problems or access problems is required to get the appropriate approvals or technicians on site to make the repairs.

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

E-Request is a new tool that automates the process for requesting access to ATF network resources. The login page will contain the same Privacy Act Statement as the manual form that this tool has replaced, the Information Systems Access Form (ATF F 7200.1):

The primary use of this information is by management and information systems administrators to approve, grant, and control access to sensitive information systems. Additional disclosures of the information may be: to a Federal, State, or local law enforcement agency when ATF becomes aware of a violation or possible violation of civil or criminal law; or to a Federal agency when conducting an investigation on you for security reasons. Where the employee identification number is your social security number, collection of this information is authorized by Executive Order 9397. Furnishing the information on this form, including your social security number, is voluntary, but failure to do so may result in disapproval of this request.

Executive Order 9397: Numbering System for Federal Accounts Relating to Individuals Persons

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.

The last 4 digits of the SSN are required. The date of birth and mother's maiden name are not required and are usually used as an alternative to the last four of the SSN. Asking for the last four digits of the SSN is the primary method for identifying a user. There are informal ways of working with individuals that are concerned about using the last 4 digits of their SSN. Regardless, this data is still protected from non-approved users from changing or viewing. Via permissions, only a select group of users are allowed to view the data to confirm who is actually making the call or asking for assistance. ATF is currently evaluating moving away from the last 4 digits of the SSN and towards a more informal method of validation (secret question and answer). An audit trail is kept for any changes to a ticket. An audit trail is also kept for changes to any of the validation information. We have encrypted and increased role-based permissions on data that was felt to be at risk. Specifically, full SSN and license plate numbers and licenses are encrypted and only users with the role-based permissions can un-encrypt. There is currently no audit log for records that are only viewed. A change must occur to capture who, what, and when.

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 contained in Remedy is used to identify callers to the Help Desk, process requests for access to resources, dispatch of field technicians for software of hardware calls, and equipment tracking.

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.)

No, the system cannot be associated to any type of Data mining system.

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

Accuracy of data is constantly updated by individuals. If location changes they can call the help desk and have the location changed. Remedy administrations are also performed periodically to import the updates to the data. Data is constantly updated once HR Connect reports are provided by the Human Resources Division. The reports are in the form of an Excel spreadsheet and are sent to the Remedy Development Team twice a week. There is no automated feed from HR Connect, and there are no other systems to validate information against. ISD provides a list of users that are to be marked as inactive on a monthly basis. That list is imported into Remedy and tickets to the Help Desk, Asset Management, Oracle and Tivoli teams are generated to cancel accounts.

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)?

Retention period is 3 years for tickets, but profiles are kept indefinitely to ensure that another user will not be assigned the same login. NARA has not approved the retention schedule. The RFI records will be kept indefinitely to insure agents have access to all history. This retention schedule has been

approved by (NARA). (Ref: ATF RCS 101, item 99-3 Remedy/E-Request System (Helpdesk Expert Automation Tool): GRS 24:Item 10b; GRS 24: Item 6a; GRS 20, Item 6).

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

User based permissions restrict the information that be can viewed or modified via the Remedy COTS work flow engine. As fields are created or exist in the Information Technology Service Management (ITSM) product suite, they are given permissions as to who can view, and who can change. Permissions are granted by the Remedy Development Team, the only administrators to the system. Only administrators have access to all data. Permissions are used to restrict access to data during the development cycle, which is when groups are created. At this point, users are unable to see the data and/or change the data. Once a field is updated/created the developers can grant permissions appropriate to the customer needs while taking into account security considerations. Prior to assigning users to a group, he/she must follow the formal request process.

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 (DOJ) and with other recipients.

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

There are no internal components of the department that data is shared with.

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

Not applicable.

4.3 How is the information transmitted or disclosed?

Not applicable.

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

Not applicable.

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?

ATF's IT systems managed service contractor Electronic Data Systems (EDS) Corporation and their sub-contractors manage the data in the Remedy System. Decision One is used to dispatch field engineers to correct workstation, servers, hardware and software problems. Decision One receives Remedy ticket information to include description of issue, city state and zip, and any asset information that may be applicable to the issue. Then they dispatch a field engineer to resolve the issue. The field engineer takes the ticket number he receives from DDG, a ticketing application, and logs in to TREO/AEROPRISE browser in order to receive the ATF SBU data (name, address and phone). The data is actually in a Remedy form that Aeroprise, a third-party vendor, displays on a Treo (handheld unit) in a usable format. The Treo browser URL goes to an ATF re-direct through the firewall. Security is in place that a user must have Remedy login, has permissions to the D1 form in Aeroprise, has permissions to the D1 form in Remedy and must be going thru the firewall from a Treo only.

5.2 What information is shared and for what purpose?

No data is shared with external agencies other than that data discussed above in regards to an EDS sub-contractor.

5.3 How is the information transmitted or disclosed?

There is no data shared with external agencies. Data is routed to and from Decision One, an external field support dispatch group, via an XML secure https push to a secure ASP page that Decision One operates.

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

ATF has non-disclosure agreements with all contractors.

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

There are no users from outside agencies with access to the Remedy System. Prior to ATF government or ATF contractor receiving access to the Remedy system they must complete an information systems access form online (E-Request) and receive approval from the Remedy System Owner.

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

Auditing occurs when a field is changed or a new entry is made. The information change or audit is written to the work log and summary fields. In some cases to see who has changed certain fields on a ticket, an audit trail tab has been constructed. Any change to the Person Information Form is captured on each record and a report can be run to show who the last person to change that record was. As mentioned previously any record can be viewed with no audit trial.

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

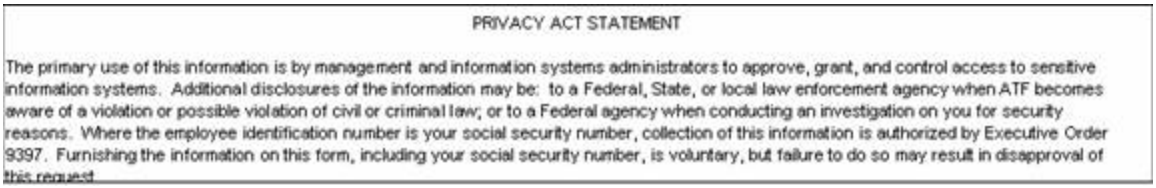
In an effort to mitigate the risk of sending an agent's name, address and phone number, ATF implemented a policy that would only allow the city, state and zip to be sent in the xml push and, therefore, no SBU data would be stored in the Decision One database. When the field engineer is notified of a ticket they would have to log into a secure web site in the ATF DMZ that would allow them to access SBU data from Remedy directly (name, address and phone).

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?

The Privacy Act Statement at the bottom of the Information Systems Access Form, ATF F 7200.1 (as shown below) will be placed on the E-Request login page. E-Request is a new tool that automates the process for requesting access to ATF network resources.



PRIVACY ACT STATEMENT

The primary use of this information is by management and information systems administrators to approve, grant, and control access to sensitive information systems. Additional disclosures of the information may be: to a Federal, State, or local law enforcement agency when ATF becomes aware of a violation or possible violation of civil or criminal law; or to a Federal agency when conducting an investigation on you for security reasons. Where the employee identification number is your social security number, collection of this information is authorized by Executive Order 9397. Furnishing the information on this form, including your social security number, is voluntary, but failure to do so may result in disapproval of this request.

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

Yes – but failure **may** result in inability to identify user. They can provide alternate identification or can have their manager provide his or her identification in the verification of the individual. The last 4 of the SSN, the date of birth and the mother's maiden name are not verified by any other systems, so if an individual wants to say their mother's name is something other than what it really is, the ATF requester just has to remember what they have given the ATF help desk as an identifier. Just like the 'secret question', incorrect data will always be possible and also requires the user to remember what their answer is. An IP-based system would not identify an ATF user; it would only identify an ATF machine. If an unauthorized user is able to gain access to a workstation, he/she can pose as an ATF authorized user assigned to that workstation to perform malicious activity.

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?

The user does not have to provide his/her mother's maiden name or birthdate. Last four of SSN is the predominate way of identifying a user. There are informal ways of working with individuals that are concerned about using their last 4 of their SSN. This includes

telling the user to provide fictitious information when asked to provide his/her mother's maiden name or birthdate.

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

Risks of compromising an individual's identity are always present but we store the absolute minimum data and only storing the last 4 of the SSN in the system. Through Remedy permissions we are protecting individuals' identities and the compromise of that information. Only certain individuals are authorized to change and see certain data. Remedy App-Management, a permission in Remedy, can allow an approved user to see the last 4 of a user's SSN and can change the mother's maiden name and birthday fields. This permission is limited and granted on an as needed basis. The Remedy Administrators will grant this permission at the request of ATF management.

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?

When a person is on the phone with a help desk technician, they have the opportunity to correct or add any address or other information they wish to have stored in their profile

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

Users may contact the Help Desk to request a change to their information.

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

At anytime a user can create a ticket by calling help desk and ask for the information that is in Remedy. Additionally, users will soon have ability to see their own tickets that have been created under their login and all data associated with those tickets.

7.4 Privacy Impact Analysis: 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.

No process at this time.

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?

Principally, ATF Information Services Branch (ISD) has access to Remedy. This encompasses the Service Management Branch, Service Delivery Branch, Product Assurance Branch, and contractor groups in support of the ATF architecture. All ATF employees and contractors must have access to Remedy and E-Request in order to request access to ATF network resources.

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.

YES, see attached

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

Yes, roles are used to allow what a user can and cannot see and do. The roles are they can write or change a field, or they can view a field or they cannot see a field. The specific roles are: view, change and hidden.

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

Yes, through E-Request a manager will request one of his new users be allowed access to Remedy. Once that request is approved by the Remedy System Owner, a ticket is created and sent to the Remedy Team to grant access. That access only includes access to E-Request so in the future the user can request his/her own application requests. An audit trail exists of who approved the accounts, and who created the accounts and who requested the accounts. If a user does not log into a specific application in a 90 day period, the account is suspended and E-request shows the account as suspended. When a user is

suspended, his/her manager can then approve him/her to be provided access again, but this time the ticket will go directly to the Oracle Team to create account and skips system owner approval.

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

Testing is done during development. E-Request is a tool (within Remedy) that automates the process for requesting access to ATF network resources, which has replaced the manual process of completing and routing the Information Systems Access form (7200.1). E-Request has undergone all Independent Verification and Validation (IV&V) Testing and User Acceptance (UA) testing. The majority of the testing focused around the roles and approvals of E-Request. There were no issues identified in the testing regarding roles.

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

Changes are captured by Remedy. Remedy's auditing includes who has accessed a ticket, any changes they made, and all changes previously made prior to current change.

Deleted tickets are captured and who deleted them as well. A log file of deleted tickets and deleted users is sent to ISSO on a nightly basis for their review. No irregularities have ever been found regarding data.

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

No additional training.

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

Yes, last C&A on Sept 21, 2006

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

In an effort to protect privacy of users, using the role-based functionality of Remedy, certain forms (Person Information Form) are only accessible by authorized individuals. The minimum amount of personal data is stored and shared. We are evaluating using a secret question and answer format. For Several applications in E-Request a complete SSN is required (N-force, N-Focus, N-Quire and N-spect).

When the full SSN is asked for, the requester must put in the full SSN that is immediately encrypted. Only the system owner can see the full SSN, via permissions previously described. We use the Remedy encryption functionality that uses a 30 character GUID as the key to encryption, that key is hidden in the database as proprietary data.

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?

No. EDS is the sub-contractor running a managed service contract for the ATF. EDS chose Remedy to implement as the trouble ticketing system as it met the ATF requirements at the lowest price to implement and maintain. EDS felt that Remedy exceeded or met all system goals and was able to implement and therefore bid at the lowest cost to ATF. A managed service contract is one where EDS is paid a price per seat.

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

ATF analyzed the managed service contract and the EDS proposal and ultimately agreed that Remedy met and exceeded all PII data storage requirements.

9.3 What design choices were made to enhance privacy?

Maximum use of roles and groups.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

Through the use of stringent roles and permissions, along with an extensive audit system Remedy has been protected from inside and outside the firewall from unauthorized access. Data is stored in tables that have permissions so only certain approved individuals can see or change data. Audit trails of those changes are captured in the system. The minimum amount of data is stored to identify an individual who is calling to ensure information is not given to an unauthorized user.

Responsible Officials

(signed)

Luis E. Vega

Chief, Operations Performance Management Section

Information Services Division

Office of Science and Technology

Approval Signature Page

(signed)

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice