System Inspection (Multi-Agency Report): Structured Data Managed within Databases

National Archives and Records Administration
November 2024

INTRODUCTION

The National Archives and Records Administration (NARA) is responsible for assessing the proper management of records in all media within federal agencies to protect rights, assure government accountability, and preserve and make available records of enduring value. In this capacity and based on authority granted by 44 United States Code (U.S.C.) 2904(c)(7) and 2906, NARA inspects the records management programs of agencies to ensure compliance with Federal statutes and regulations and to investigate specific issues or concerns. NARA then works with agencies to make improvements to their programs based on inspection findings and recommendations.

This inspection was performed to provide objective analysis, findings, and recommendations to assist the participating agencies with governance and oversight to:

- Review and assess database processes and policies.
- Assess migration and operations and maintenance.
- Transfers to NARA and sunsetting of particular databases.

For this inspection we reviewed agency documentation that included RM policies, system configuration plans, previous internal audits, security plans and data recovery plans. Additionally, we saw database demonstrations where we were able to compare the documentation to real practices. The majority of the evidence was collected through interviews that were conducted virtually. We evaluated performance and compliance against the Federal Records Act, NARA's implementing regulations in 36 C.F.R. Chapter XII, Subchapter B, NARA Bulletins, NARA's Electronic Records Maturity Model, and the U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book).

This report addresses how five selected federal agencies manage their permanent electronic records in databases or content management systems. Furthermore, this report will detail how the technology of the database assists or hinders the records management (RM) process. This inspection report only reflects what NARA's staff saw and heard at the time of the interviews. The documentation review and inspection interviews were conducted between August and December 2023 with database demonstration sessions happening in January 2024. Any changes to their databases since the interviews will not be reflected in this inspection report.

The participating agencies were:

- Administration for Children and Families (ACF)
- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- United States Parole Commission (USPC)
- Institute of Museum and Library Services (IMLS)
- United States Department of Veterans Affairs (VA)

OVERALL OBSERVATIONS

Our general takeaway from this inspection is that the agencies that are actively using their databases for day-to-day business are managing them well from a records management (RM) and information technology (IT) standpoint. Through documentation, we learned that some of the databases were inactive. Some were formally decommissioned, while others are in a stagnant holding pattern. The active databases have retention schedules and attention from the agency's RM staff. Additionally, they are on current or near current versions of industry-standard database platforms such as those by Oracle and Microsoft, for example. IT processes including maintaining backups, conducting tests, migrating to a cloud environment, or maintaining security controls are in place for all the active databases.

RECORDS MANAGEMENT

Most agencies and program offices that were inspected manage their systems efficiently. The AROs provided records management policies, prior to the interviews. We found that most of the systems inspected were in the cloud. For those that were not, some were scheduled to migrate to the cloud in the current calendar year. There were databases that were scheduled to remain enterprise-based for the foreseeable future. Our observation is that cloud migrations were happening at the agencies at a departmental level and in most cases, they were being migrated to a larger content management cloud-based system that would allow for greater security and management over all databases and systems within the department. We found varying degrees of how much RM is involved in the migration process. Many agencies treat the migration of the databases as solely a technical exercise, thus only having the information technology office or branch involved and did not include much input from the Senior Agency Official for Records Management (SAORM), Agency Records Officer (ARO) or RM staff.

All the databases had at least been migrated once from an on-premises system. Many are on their second or third migration within 20 years. The AROs are confident that the established risk management plans have been sufficient to ensure that proper records management has taken place throughout system migrations.

SYSTEM DESIGN & IMPLEMENTATION

Overwhelmingly, the databases we inspected were commercial-off-the-shelf (COTS). Nevertheless, they varied in platform and design language. The understanding from the interviews was that COTS products allowed for easier maintenance, compatibility with other systems and easier knowledge sharing among users and information technology professionals.

OPERATIONS & MAINTENANCE

The security of the database and the records within were deemed very important by all participants in this inspection. Security patches were usually pushed on a scheduled basis to the database. Those within the cloud used the host-provided security patches. Patches were usually pushed on a monthly schedule but would be done more frequently or on an ad hoc basis if needed. Security was exclusively handled by the information technology department of the agencies.

OVERALL FINDINGS AND RECOMMENDATIONS

The following are general global observations or themes that emerged from our interviews and documentation provided by the agencies:

Overall Finding 1: Agencies need to transfer their permanent records to NARA in accordance with the approved schedule. (§ 36 CFR 1235.12)[1]

Each database inspected currently has an approved records schedule stating that all permanent records should be transferred to NARA on a specific timeline. According to § 36 CFR 1235.12 (b), records in existence for longer than 30 years are eligible for transfer to NARA. This may apply to certain record sets too.[2] The majority of the records in these databases have never been transferred to NARA or the records transfers have significant gaps. Many databases have recently been completed or are currently planning a migration to the cloud or a new database management system, which has hindered their transfer to NARA.

Overall Recommendation 1.1: Agencies should incorporate records management and transfer to NARA in their database migration planning and implementation.

Overall Recommendation 1.2: Migration to the cloud adds complexities that should be considered and mitigated so that records are validated and can then be properly transferred to NARA on their respective schedules.

Overall Finding 2: Record schedules need to be updated. (36 CFR Part 1225.22)[3]

A common theme that arose during the inspection was that agency records officers and/or program officers were not sure if the records schedules were up to date. Oftentimes, the record schedule was created by a predecessor, and since then, the schedule has not been updated. With a few exceptions, most of the schedules date back to the 1990s through the early 2000s. Many of the descriptions of the systems are out-of-date. The AROs are maintaining the records using the schedule, but it may not be optimal for their current workflow and needs. Some AROs need to gain a better understanding of the record sets before they can adequately write new schedules. In a few instances the AROs were unaware of necessary information that was crucial to understanding the record sets.

In addition to the schedules, many of the AROs were not aware or part of database migrations to the cloud. Understanding this is a technical aspect, the IT teams at these agencies took the lead. However, because it deals with records, the AROs should be included in this process.

---

[1] "§ 1235.12 When must agencies transfer records to the National Archives of the United States?" 2009. eCFR. https://www.ecfr.gov/current/title-36/section-1235.12.
[2] 36 CFR Part 1235 -- Transfer of Records to the National Archives of the United States. (2009). eCFR. Retrieved February 1, 2024, from https://www.ecfr.gov/current/title-36/part-1235#p-1235.12(b).
[3] 36 CFR 1225.22 -- When must agencies reschedule or review their records schedules? (2009). eCFR. Retrieved February 2, 2024, from https://www.ecfr.gov/current/title-36/chapter-XII/subchapter-B/part-1225/section-1225.22.

Overall Recommendation 2: AROs should be made aware of any system migrations to ensure that RM is part of the process of migration. This would promote consideration of potential RM issues prior to any migration or change to the current state of the database.

Overall Finding 3: Agencies must notify NARA when a system is inactive. (36 CFR Part 1225.22)[4]

During the interview process we found out that a few of the systems under inspection are offline and inactive. While conducting our preliminary research for this inspection we found no indication that any of the systems we had chosen to inspect were inactive. We found on multiple occasions that systems were decommissioned or merged without notice and without transfer of records. In some instances, the decommissioned system was encapsulated with another system and therefore the records are safe and being managed despite being combined with another disposition authority.

Overall Recommendation 3: Inactivity must be reported to NARA, so records schedules can be updated. Additionally, permanent records should still be transferred to NARA prior to system decommissioning.

NOTEWORTHY PRACTICES

The following are best practices that are worth consideration for all agencies that were part of this inspection:

Noteworthy Practice 1: Including RM in System Planning and Implementation

The ATF's ARO sits on the agency's technical review board where they make decisions regarding the agency's IT infrastructure. The ARO brings the perspective of records management to the IT discussions. Oftentimes, IT decisions are made and implemented without the inclusion of RM. There is a risk posed when a system becomes operational, and no RM ramifications are considered. This can lead to a flaw in RM capabilities or potentially no RM capabilities at all. ATF including the RM staff during the planning and implementation phase is a great practice that supports maintaining quality records.

Furthermore, the ATF's ARO signs off on any system before it is decommissioned by the agency. The ARO checks to ensure that all RM responsibilities are taken care of before the system is decommissioned. This ensures that no records are mistakenly lost, and disposition follows the records schedule.

Noteworthy Practice 2: Review of Records

The National Cemetery Administration (NCA) of the Department of Veterans Affairs (VA) had a unique policy for managing revisions to records that we did not see at other agencies during this inspection. The NCA's Burial Operations Support System (BOSS) database requires two levels of review before any record can be revised in the database. The records can only be entered through

[4] § 36 CFR Part 1225.22.

the database's user interface. Once the record has reached a certain stage in the workflow process the record is basically locked from any changes. A revision can be requested but the change has to be approved by users with administrative privileges in the database. Having multiple levels of review for a record to be changed ensures data integrity of the record.

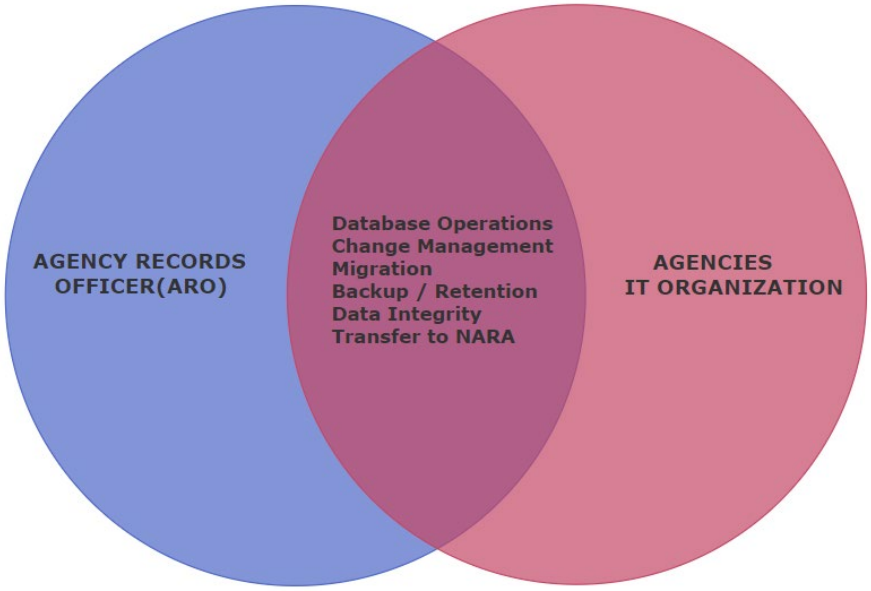
Noteworthy Practice 3: Segregation of Records

NCA's BOSS and Automated Monument Application System (AMAS) databases have entries from state and private cemeteries in addition to the federal run cemeteries. Each State and US Territory has its own partition of BOSS/AMAS, which allows it to enter data regarding veteran burials and applications. A good practice in RM and IT governance is that only the state or territory can enter, view and revise data that is a part of its own state or territory. This protects the integrity of the data, and if an IT incident such as virus or corruption of data occurs it will not affect the larger dataset.

CONCLUSION

In conclusion, through inspection interviews and review of data/documents, we found that there is a wide range of database records across the agencies. In addition, there are broad ranges of technical platforms, architecture, and histories of each database. Many of the databases had been migrated from prior data, while others were new concepts that needed to be put into a system to manage or disperse data in a meaningful way. The functions and purposes of each of the databases were unique, ranging from internal agency use, to having external stakeholders sharing and adding to the records.

RM should be considered in all aspects of the database lifecycle. AROs should work with their agency's IT departments to ensure that data integrity is part of all migrations and other aspects of database operations.



Including AROs and other RM staff in the IT-related conversations brings RM concerns to the discussion. This is something that agencies should continue to strive for and adapt to as IT infrastructure modernizes and changes.

AROs and RM should be at the forefront more so than ever as many of these databases are leveraging cutting edge cloud platforms. This environment is complex and evolving, requiring agencies to protect, secure and maintain records in these and every recordkeeping system.

AGENCY TECHNICAL SUMMARY

ADMINISTRATION FOR CHILDREN AND FAMILIES

In this report we inspected two databases from ACF. The first one is from ACF's Office on Trafficking in Persons (OTIP), which is called Shepherd 1.0. The second is named Regional Partnership Grants Evaluation Data System (RPG-EDS).

Shepherd 1.0 Database Introduction

The primary function of the Shepherd 1.0 solution is to electronically process certification and eligibility determinations for potential victims of human trafficking. The technology solution should allow for the electronic submission of adult immigration documentation, child eligibility Request for Assistance forms, and all other associated paperwork through a public web portal. All forms and documentation would then be electronically parsed, stored, managed and routed through OTIP and relevant parties to increase the speed of determinations. This would lessen the amount of manual data entry required and greatly expedite the overall Adult Certification and Child Eligibility processes to allow HHS to serve victims of human trafficking and meet legislative mandates as expeditiously as possible. Later, as part of a separate project, Shepherd was integrated as a module into a new system called ATIMS (Anti-Trafficking Information Management System).

Technical Details Shepherd 1.0 Database

The Shepherd 1.0 runs on AWS RDS SQL ServerSQL, Server Databases, which is hosted in the secure ACF Amazon Web Services (AWS) cloud-computing platform. The technology components used to interface with this database are Web Server IIS, .NET core, Windows Server 2016, and SMTP.

The database design provides metadata and classification techniques for identifying and classifying records. Data is encrypted both in transit and at rest.

Shepherd deploys multiple security mechanisms to secure its communication, data, and infrastructure. Shepherd uses HTTPS protocol to transmit data over the internet. The data transmission is completely encrypted and secured through trusted security certificates. Users log on using two-factor authentication, and documents uploaded to Shepherd are scanned for viruses and malware. ACF conducts periodic security scans to ensure that the system remains secure.

Shepherd accounts consist of internal users including system administrator, case specialist, case approver, data analyst, DHS document submitter. External users include case requester, certification specialist, TVAP service specialist, NGO consultant, law enforcement consultant, account managers, group, and role membership, along with access authorizations/privileges assigned for each type of account. Users must comply with all system usage rules of behavior.

Shepherd utilizes site restoration in case data is accidentally deleted, altered, or lost. Backups are done incrementally and in full and taken every 4 hours to mitigate against any data loss.

RPG-EDS Database Introduction

RPG-EDS serves the ACF of the Department of Health and Human Services (HHS), stakeholders, and users. The purpose of RPG-EDS is to support families in which a child is in or at risk of out-of-home placement because of a parent's or caretaker's substance use disorder. The Children's Bureau (CB) developed RPG- EDS for grantees to use for collecting and reporting on their performance and progress, such as services and client outcomes. CB uses the data to monitor grantees' progress and to conduct a cross-site evaluation of grantee services, partnerships, and client outcomes.

Technical Details of RPG-EDS Database

RPG-EDS is hosted on the Microsoft Azure Government Cloud Platform leveraging Platform-as-a-Service (PaaS) offerings. The Microsoft Azure Government Cloud Platform is IPV6 enabled.

RPG-EDS uses the following tools:

• Azure Portal – Cloud services management
• SharePoint – Artifact/Document management

Records management requirements are incorporated into the system design documents and validated at implementation. In addition the design provides metadata and classification techniques for identifying and classifying records. Standardized information input, data validation rules, and controlled data uploads are safeguards in place to guarantee precise record capturing classification during data entry. Encryption is used to secure data in transit and at rest.

Audit trails and logs are used to monitor access, revisions and other records management related activities. The database maintains adequate metadata as defined in NARA Bulletin 2015-04[5], and the database allows users to perform a full text search.

Security patches are regularly applied to the system. Access controls are necessary to ensure correct operation and security of the system. Access controls for the RPG-EDS encompass assigning and maintaining user's roles, requiring users to change passwords, and adding or removing application access. Access controls are managed directly through the RPG-EDS web application through the User Administration webpage.

Policies that ensure access rights, permission rules and controls for electronic records are routinely updated. The system does support searching in response to information requests including FOIA. All data is stored in the live database. No migration has been performed or is planned to be performed in the future.

Records for ACF databases are not ready for transfer to NARA according to their records schedule. They have been up to date with their current block of records for 5 years. ACF stated

[5] Bulletin 2015-04. (2015, September 15). National Archives. Retrieved January 24, 2024, from https://www.archives.gov/records-mgmt/bulletins/2015/2015-04.html.

they have had issues in the past transferring records to NARA using e-transfer. ACF could not connect to NARA using the File Transfer Protocol. They were able to find a workaround and transfer the records directly through the Electronic Records Archive 2.0 (ERA 2.0).

Findings and Recommendations for Shepherd 1.0 and RPG-EDS

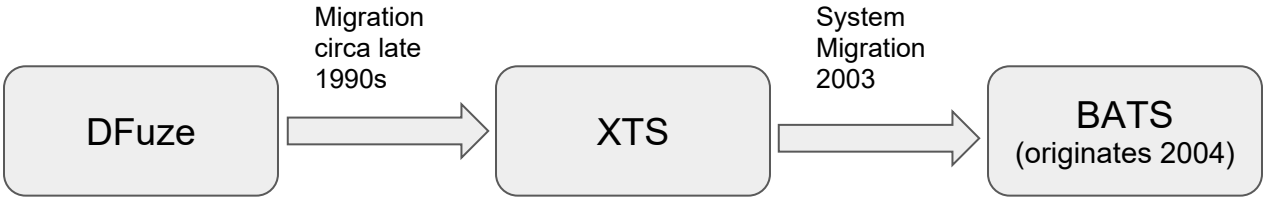
Finding 1: Backup schedules are neither routine nor clear for RPG-EDS.

Backups are an essential aspect of retaining the integrity of records. They also ensure that vital records are adequately protected against any adverse events of data loss. A backup retention schedule should be executed on the database to ensure that data is safe and can be recovered.

Recommendation 1: ACF should clarify their database backup schedule. If a backup schedule is not in place, a backup retention schedule should be created to protect the records in the system. (36 CFR 1223.14(d))

THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS AND EXPLOSIVES

In this report we studied the ATF's Bomb Arson Tracking System (BATS) database, and its two predecessor systems, the Explosives Tracking System (XTS), and DFuze. We also reviewed the Firearms Tracing System (FTS) database.



BATS Database Introduction

The BATS database is designed to store information related to public safety concerns surrounding the use of explosive devices. It incorporates geospatial information to record the location of all documented incidents involving explosives.

Technical Details for BATS

The system design and implementation details of the BATS database is a SQL Server 2019 database running on Windows Server 2016. Modernized access to the database is in development and will likely be built upon the .NET framework. The database resides on the AWS GovCloud and the servers are leased as a service. The AWS GovCloud is considered part of the ATF's active directory. The System Development Life Cycle (SDLC) for the system is managed as part of an Enterprise Architecture (EA) framework. RM requirements for retention, access and transfer are not part of the COTS system components, however, there is an interdisciplinary team of RM staff who ensure that RM requirements are accounted for. BATS incorporates the use of Splunk for its network security, a security auditing application. It maintains logs and acts as a monitoring tool. The BATS database operations and maintenance consists of the ATF security team regularly scanning the database servers for security vulnerabilities and categorizing them into high, medium, and low impact with a set timeframe for mitigation to be put in place.

All geospatial information can be generated by any team; it is all considered temporary data until it is specifically attached to a case file, at which point the data becomes permanent. Reused geospatial data is stored in libraries that have a temporary retention schedule. The geospatial information in BATS is stored in Esri ArcGIS. BATS is a "no delete" system. Once a record is closed it cannot be changed or deleted. As it is only public safety hazard information that is maintained in BATS, routine mining operations use of explosives would not be recorded in the system.

There are role-based access permissions in BATS, but they are not tied specifically to active directory. All ATF users are required to use a PIV card to authenticate to BATS; state and local users use a username and password that expires every 60 days and has strict requirements for password strength. An active Hazardous Devices School (HDS) certification is required for

access, representing another layer of access control. HDS is a bomb technician school that is run by the Federal Bureau of Investigation (FBI).

Images and PDFs can be attached and stored as database Binary Large Objects (BLOBS). The binary data can be transferred to NARA. Also transferred to NARA will be data dictionaries and entity relationship diagrams (ERDs) to explain the data. In addition to storing unstructured binary data, the system allows all lists of predefined values to be updated from within the application. This allows information to be categorized in new ways as requirements change. As there are Development, Test, Training and Production environments that are active for BATS, an infrastructure exists for making changes to the system beyond the existing system flexibility.

Records Management Details of BATS

With regards to records management of the BATS database, we identified that it is the current and active system, brought online after its predecessor, XTS, was decommissioned in 2017. Parts of the records control schedule for the database are out of date as the system is currently in flux after being moved to the cloud. The most recent transfer of BATS to NARA was in 2002. NARA accepted physical and legal custody of the records.

Upon reviewing the system documentation we received, we found that best practices for classifying records are present in the BATS System Security and Privacy Plan (SSP). This includes an assessment of information types for confidentiality, integrity, and availability into High, Medium, and Low impact categories. Information types identified are Citizen Protection, Crime Prevention, Criminal Apprehension, Criminal Investigation and Surveillance, Leadership Protection, and Property Protection. Of these, the majority are categorized as Moderate, with several categorized as Low and a few High impact. Additionally, the SSP clearly identifies system Owner, Authorizing Official, and Security Officials.

BATS is a “no delete” system. Once a record is closed it cannot be changed or deleted. Records can be disabled, for example, if the record is incomplete or there were critical errors with the entry. The disabled record still is not deleted as it stays in an “open” status. Once the record moves to a certain stage it is considered “closed.” Only closed records are counted in their national statistics and only closed records are permanent and transferred to NARA. Images can be attached to any record in the database. These images are transferred to NARA with the larger data set. However, there are questions surrounding the organization of the images in relation to the record it is attached to. There can be a separate mass export of the images from the database. Since records to NARA must be transferred in a flat file format the images will be separated. The question that arose is, can the linkage be maintained between the dataset and the image if the image is now in a separate folder?

The DFuze database (which was the predecessor to XTS and BATS) is offline due to security issues, and the data is no longer accessible and has not been transferred to NARA. DFuze was decommissioned after security patches were applied to address vulnerabilities that rendered its records inaccessible. The particular vulnerability was the Bloodhound Wind attack which could allow an unauthenticated user to execute arbitrary code on the server. Additionally, it was a COTS product which ATF stopped paying for license or support. Furthermore, after the decommissioning, we could not confirm if the records were migrated in full to BATS or if BATS

began as a point forward system with the information that was previously in DFuze. At the time the interview had taken place, ATF was working with the contractor who created DFuze to see if they could get the records of the system and transfer them to NARA.

After reviewing the DFuze system documentation, we found that best practices for classifying records are present in the DFuze user's manual. It refers to all database information as records and details that security levels for records are integrated into individual user accounts and individual records on a scale ranging from 0 to 5, corresponding to unclassified to top secret. Additionally, Administrator user's manual contains specific instructions for managing View, Add, and Delete permissions to records. It does indicate that deleting records will delete them from the "virtual store" and not from the DFuze database itself.

ATF has a full-time Records Manager on staff and the SAORM is at the DOJ headquarters level. The system owners are responsible for Records and Information Management (RIM) certifications (RIMCert). There are both federal employees and contractors (project managers) with RM responsibilities. Both federal and state employees have creation and editing access in the BATS database. There is no RM training program in place, however, state, local and tribal government users agree to Rules of Behavior. The database does support searches in response to FOIA requests. There is a control for records in the system that prevents records from being deleted.

Regular system-wide vulnerability assessments are conducted. A RIMCert process is in place to meet the requirements of 36 CFR for unauthorized access, disposition, and modification of records. Most of the system users are outside ATF, and all agree to Rules of Behavior (ROB) for accessing the system to help protect records. Access rights and permissions are role based. Everyone with access to the system has write access, with the only exception being people classified as working in intelligence. The records are expected to exist beyond the lifetime of the current system implementation, and a migration plan is in place for ultimately migrating records to any future system. Any new system components brought online will have a Requirements Traceability Verification Matrix (RTVM) developed, which maps all test cases to RM system requirements.

FTS Database Introduction

The Firearms Tracing System (FTS) database is designed to support the firearms component of the ATF's mission. It is used by the National Tracing Center (NTC) to "record and review firearm trace, multiple sale, suspect gun, demand data, interstate theft, and federal firearms license theft information. The underlying database is further used to analyze crime and firearm distribution trends and to generate investigative leads."[6]

[6] Firearms Tracing System (FTS). (n.d.). National Archives. Retrieved February 12, 2024, from https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0436/n1-436-96-004_sf115.pdf.

Technical Details of FTS

The FTS system consists of an Oracle database and a Windows application built using Oracle Forms/Reports 6i with Patch 16. The FTS system design as implemented has the database residing in the cloud on a FedRamp approved platform and uses an active directory for single sign on. The scans of firearms records contained in the database are verified to ensure that every page is captured. Multiple search criteria are allowed, and the search capability is driven by the user requirements. Operationally, there are over 300 controls in the system security package, and the system's controls are reviewed twice a year. Privacy impact assessments are conducted every three years, and the system is patched every week for security. DOJ conducts privacy assessments. With regards to 36 CFR requirements for disposition, access and alteration, the system is designed so that records cannot be deleted; they can only be edited through a change review process. Additionally, an audit trail of changes is maintained. Full and incremental system backups are done on a regular, ongoing basis. As the information contained in this database is intended to be preserved permanently, it is expected that the information will outlast the current system implementation.

With regards to system testing and policy, there is an RTVM that maps all test cases to RM requirements. Automated system testing is in place, as is a policy to ensure that access rights and permissions are kept up to date. The system does support the ability to be searched in response to a FOIA request. All the information is contained in the live database. Data migration has been performed within the last twelve months and there is an active data migration plan.

The FTS System Security and Privacy Plan (SSP) begins with an assessment of information types for confidentiality, integrity, and availability into High, Medium, and Low impact categories. Information types identified are: Central Records and Statistics Management, Personal Identity and Authentication, Citizen Protection, Crime Prevention, Criminal Apprehension, and Criminal Investigation and Surveillance. Of these, the majority are categorized as Moderate, with none classified as High. Additionally, the SSP clearly identifies system Owner, Authorizing Official, and Security Officials.

The FTS system requirements document identifies a verification scenario for each system requirement, including requirements for records handling. Also, FTS has an IT Contingency Plan that is thoroughly documented.

The FTS User's Manual refers to all database information as records and contains instructions to the user such as: (1) Records are not "deleted" using the Decode module – they are only deactivated. Once a record has been marked as "inactive," it cannot be "reactivated" through the Decode subsystem. (2) Updates to records are reflected in the audit history module with the most recent update displayed at the top of the list of changes.

Records Management Details of FTS

Records are scheduled, and the records are up to date; however, none have yet been transferred to NARA. RM responsibilities have been assigned to the program office responsible for FTS. All records in the system are permanent. A SQL query can output a flat file suitable for transfer to NARA when eligible. No code lists will be transferred at that time, only actual data, however,

there is some metadata maintained in the database. FTS is a relational database with six modules that comprise the system. All six are permanent and will be transferred to NARA. Since they will be transferred as flat files, we are unable to determine how the data will be presented and how useful it will be to researchers. The scans in the database are scanned to an unknown specification and do not have optical character recognition (OCR). The scans are also placed in the ATF's Firearms Licensing System (FLS). FLS is a scheduled system with permanent records to be transferred to NARA (N1-436-94-001).[7] We did not ask questions about FLS in this inspection. Additionally, we did not get any technical information as to how FLS is technologically connected to FTS. The scans can be exported out of FTS in a similar fashion to BATS. Like BATS, FTS has the same issue with the linkage of the images outside of the active database.

Findings and Recommendations for the BATS, XTS and DFuze Databases

Finding 1: The DFuze records are currently inaccessible.

The records from the now defunct DFuze Database cannot be accessed or retrieved. ATF is working with the former contractor of the database to determine if the records can be retrieved.

Recommendation 1: ATF must retrieve, inventory, and transfer the records to NARA. If the records cannot be retrieved, ATF must report the loss to NARA as an unauthorized disposition (UD) of records.[8] [9](36 CFR Part 1230)

Finding 2: Image files cannot be exported from BATS and associated with related records.

A mass export of images from the dataset of BATS is possible but it is unclear if or how the linkage to the original record is maintained since the file format calls for a flat file when transferring to NARA.

Recommendation 2.1: ATF should conduct test exports and/or transfers before they attempt to transfer BATS records to NARA to determine how the linkage is maintained for images to the dataset. (36 CFR 1236.14)

Recommendation 2.2: ATF should consider using a Globally Unique Identifier (GUID) to identify images and associate them with records and develop a utility to extract images and write them to a file system where the GUID is part of the file path for transfer to NARA.

[7] Office of Compliance Operations: Firearms Licensing System (FLS). (n.d.). National Archives. Retrieved February 1, 2024, from https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0436/n1-436-94-001_sf115.pdf

[8] NARA's Unauthorized Disposition Reporting Requirements. (2017, November). National Archives. Retrieved February, 2024, from https://www.archives.gov/files/records-mgmt/resources/ud-submission-instructions.pdf.

[9] Unauthorized Disposition of Federal Records | National Archives. (2016, October). National Archives. Retrieved February 12, 2024, from https://www.archives.gov/records-mgmt/resources/unauthorizeddispositionoffederalrecords.

Finding 3: BATS, XTS and DFuze records have not been transferred to NARA in accordance with their schedule.

ATF has not transferred the records for these databases in the timeframe required by the records schedule. XTS and DFuze are decommissioned, and those records need to be transferred before the schedule can be updated.

Recommendation 3: ATF must transfer all their outstanding records to NARA. Both XTS and DFuze need to be transferred for the final time. (§ 36 CFR 1235.12)

Finding 4: Multi-Factor Authentication for External Users

External users of BATS, such as state and local government users, do not have a multi-factor authentication login procedure. Ensuring that records are available only to authorized users helps to protect the confidentiality and integrity of the records. A multi-factor authentication process would help to protect records in the event of a breach of username and password information.

Recommendation 4: ATF should consider implementing multi-factor authentication in the form of an access card, biometrics or some other form of hardware token for authorized users outside of ATF, such as state and local users. (§ 36 CFR 1236.10)

Finding 5: Limits of BLOB Storage Should Be Established

We did not find that the limits of very large attachments to records, stored as BLOBs, have been established as adequate for very large objects such as video or other forms of multimedia. NARA may not be able to accept records beyond certain size limitations and therefore the maximum size of information to be transferred must be identified in advance of any scheduled transfer date.

Recommendation 5: ATF should investigate the limits of BLOB storage to see if they are adequate for very large objects such as video or other forms of multimedia. (NARA Transfer Guidance, 36 CFR Parts 1235 and 1236)

Findings and Recommendations for the FTS Database

Finding 6: FTS records have not been transferred to NARA in accordance with their schedule.

The last transfer of FTS is for a series between 1989 - 1999. NARA is missing the record set between 2000 and 2021.

Recommendation 6.1: ATF should conduct a gap analysis of the FTS Records.

Recommendation 6.2: ATF must transfer all their outstanding FTS records to NARA in accordance with their records schedule. (§ 36 CFR 1235.12)

Finding 7: FTS Oracle Version is Old and Unmaintained (2007)

The backend database for FTS is built using an older version of the Oracle database, 11g, which

received its last update in 2008. Keeping software repositories such as databases on maintained versions of the software helps ensure the confidentiality, integrity and availability of records by enabling the latest security vulnerabilities to be patched.

Recommendation 7: Consider upgrading the underlying database from Oracle 11g to a newer version of Oracle or another currently supported database. (§ 36 CFR 1236.10)

DEPARTMENT OF VETERANS AFFAIRS - NATIONAL CEMETERY ADMINISTRATION

BOSS Database Introduction

The Burial Operations Support System (BOSS) database is utilized by the National Cemetery Administration (NCA) to manage and process records and forms for over 100,000 burials, across cemeteries, including National, State Veterans military, Department of Army and Department of Interior (DOI) cemeteries. The Automated Monument Application System (AMAS) was developed to track the procurement, ordering, and replacement of government-provided monuments for the graves of deceased Veterans. At that time, both BOSS and AMAS ran as two distinctly separate systems, with BOSS supplying support to national cemeteries and AMAS providing support to the Memorial Program Service (MPS).

In 1996, AMAS data was merged into the existing Burial Operations Support System Enterprise (BOSS-E) database structure, and the interface was redesigned to serve out either a BOSS user interface or an AMAS user interface depending on the user's role. Merged into a single system, it is now referred to as BOSS-E. BOSS-E systems maintain approximately 8 million Veteran and dependent records and processes, approximately 150,000 burials, and over 350,000 headstone and marker orders annually. In the subsequent years, several additional applications were created and integrated into the BOSS-E system (Systems Engineering Assessment for NCA Legacy Systems).

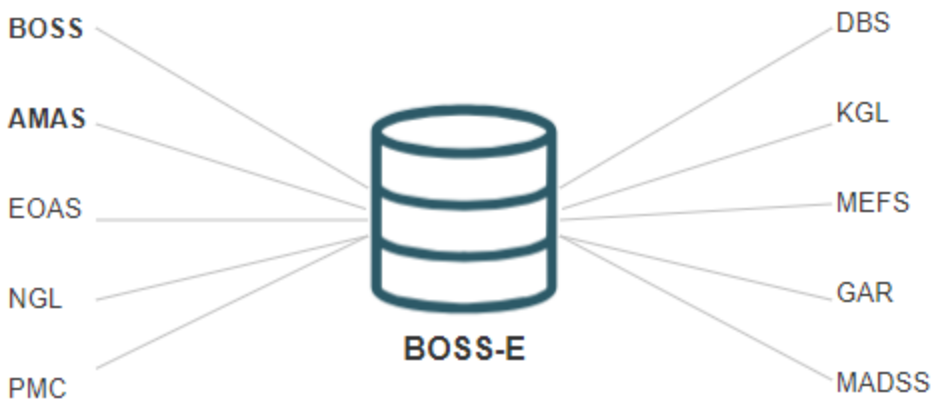
Technical Details of BOSS

Both databases, BOSS and AMAS run on management platforms operating on Oracle, Red Hat Unix, and IBM P-Series. The technology used to interface with the database is Weblogic. The System is housed in the AWS cloud with a FedRamp approved high security rating. A forms-based interface is used to interact with the database and reports are generated using C and Java computer programming languages. The design has undergone a formal VA Enterprise Architecture approval process from the product owner, The Office of Information Technology (OIT). RM requirements for retention, access and transfer are incorporated in the initial system design and validated as being present in the actual implementation. Two factor authentication is not currently supported in BOSS; however, a PIV card is used for identity. Audit trails are used to log access and revisions to data. Twice annually there is a review for access rights to the database.

The database is regularly updated to protect from security threats and any other vulnerabilities, and vulnerability assessments are conducted. With regards to 36 CFR guidelines for retention, access and modification, the database is compliant. Records in the database can only be managed through the application's user interface and two levels of approval are needed to change, alter or modify records. Deletion of records is not allowed. The IG reviews the records every six months. As for obtaining access rights to the system, users must request them by submitting a 99-57 form which requires two levels of approval. The records in the database will continue to exist beyond the lifetime of the current system implementation. Backups are performed with a nightly incremental and weekly full schedule. Restore testing was done during the last database upgrade. The migration to the AWS Cloud took place in December 2022, in which completeness of records was verified by checksums. Prior to its migration to the AWS Cloud, BOSS was an on-premises database housed in Quantico, Virginia. The migration was handled by the OIT System Administrators team. Versions of the records were maintained by Oracle database utilities.

Testing is performed as part of an agile development process every two weeks. Testing is manual and a release manager develops the test scripts. Although not part of the system's SOP, there is an annual regression test performed. The Change Control Board (CCB) meets weekly with actions documented in Jira. Jira Service Management eases the intake of changes with an intuitive service desk and automation for risk assessment and approval routing. Requirements Traceability Verification Matrix (RTVM) is documented as part of the JIRA framework. Penetration tests are conducted every 6 months with the last full system regression test being performed during the database system migration to AWS Cloud.

BOSS-E is a system of systems consisting of ten VA legacy sub-systems. BOSS and AMAS are connected to the National Gravesite Locator (NGL). The records that are created in BOSS and AMAS have certain fields that can be searched in NGL. NGL and Kiosk - Nationwide Gravesite Locator (KGL) are public systems that allow the public to search the location of a buried veteran.



The database can be searched to support business needs and FOIA requests, however, these searches need to be performed by a system administrator. There is no archive or cold storage for the data, it is all contained in the live database. There are extensive backup and restore procedures in place. Reports demonstrating compliance with requirements are produced for the IG. The system has a proposed sunset date of 2028, at which time the tentative plan is to migrate it to Salesforce.

Records Management Details of BOSS

At the time of the interview, there had not been a transfer of BOSS records to NARA. NARA should have received records from 1993 through 2022 for BOSS and from 1994 through 2022 for AMAS along with its corresponding documentation. BOSS and AMAS are relational databases and, according to representatives from NCA, they cannot be exported and transferred as flat files. According to NARA's Transfer Guidance bulletin, NARA Bulletin 2018-01, which specifies the file formats that are acceptable when transferring permanent electronic records to NARA,

structured data files need to be transferred flat.[10] [11] NARA does have the exception which utilizes Software Independent Archival of Relational Databases (SIARD) and transfers can be made in the SIARD-2.2 Format Specification. SIARD is an open file format for the long-term archiving of relational databases in the form of text data based on XML that are packaged in a container file.[12] Despite SIARD being an option, NCA is not allowed to use it for internal security and operational reasons.

BOSS-E is an enterprise version that encompasses multiple databases of NCA in addition to BOSS and AMAS. We did not go into detail about BOSS-E in the interview, but with further research after the interview, we discovered this in the documentation the agency provided. Besides BOSS and AMAS, we are unsure if the other records are temporary or permanent. There is not a current records schedule for BOSS-E, nor is there a separate schedule for some, if not all, of the components of BOSS-E.

Findings and Recommendations for BOSS/AMAS:

Finding 1: BOSS and AMAS would benefit from a two-factor login process.

The absence of a two-factor login for the records database presents a security concern. Without this authentication step unauthorized individuals might gain access to the database resulting in data breaches and violations of regulations. Ensuring that records are available only to authorized users helps to protect the confidentiality and integrity of the records. A multi-factor authentication process would help to protect records in the event of a breach of username and password information.

According to VA's Information Technology, two-factor authentication is in the process of being implemented. However, they must retire their Feith software first. Feith is scheduled for decommissioning in 4th quarter 2024.

Recommendation 1: Implement a two-factor login to safeguard the confidentiality, integrity and availability of the records while also adhering to regulations. (36 CFR 1236.10(b)) (ISO 15489-1:2016, Section 9.5 Access control)[13]

Finding 2: NCA cannot transfer these records to NARA.

Structured data files need to be transferred to NARA in accordance with NARA Bulletin 2018-01. That bulletin states that records must be transferred as flat files or in a SIARD 2.2 format. NCA can do neither.

Recommendation 2.1: NCA must determine how to transfer BOSS and AMAS records to NARA.

---

[10] NARA Transfer Guidance. (2023, September 8). National Archives. Retrieved February 5, 2024, from https://www.archives.gov/records-mgmt/policy/transfer-guidance.html.

[11] Appendix A: Tables of File Formats. (2023, September 8). National Archives. Retrieved February 12, 2024, from https://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html.

[12] SIARD Format Specification. (2021, August 31). SIARD. Retrieved February, 2024, from https://siard.dilcis.eu/SIARD%202.2/SIARD%202.2.pdf.

[13] INTERNATIONAL STANDARD ISO 15489-1. (2016, April 15). iTeh Standards. Retrieved February 8, 2024, from https://cdn.standards.iteh.ai/samples/62542/fe383f4fe10448d5b22ce628b1542ed6/ISO-15489-1-2016.pdf.

They will need to work with NARA's Electronic Records Processing Branch to determine if there are alternatives and/or how they may be able to transfer the records to close the gaps. (NARA Bulletin 2018-01)

Recommendation 2.2: NCA must transfer outstanding BOSS and AMAS records to NARA. (§ 36 CFR 1235.12)

DEPARTMENT OF VETERANS AFFAIRS - VETERANS HEALTH ADMINISTRATION

Environmental Agent Service Registries Databases Introduction

The Environmental Agent Service Registries (EAS/R) is a combination of application inputs for the Ionizing Radiation Registry (IRR), the Agent Orange Registry (AOR), and the Gulf War Registry (GWR) at the Veterans Health Administration. EAS/R is used to record, track, and monitor the health of specific groups of Veterans. It provides a mechanism to catalog prominent symptoms, reproductive health, reported exposures and diagnoses. For this inspection, our prime focus was only on IRR and AOR.

Environmental Agent Service Registries Databases Technical Details

EAS is hosted at the Austin Information Technology Center (AITC). These servers fall under the authorization boundary of the Infrastructure Operations (IO) UNIX and Windows Service Lines. The platform for the database is Oracle 19c running on Linux, and the applications connect by ODBC. There is an enterprise architecture in place for the system design, and RM requirements for retention, access, and transfer are incorporated into the system design and validated as present in the actual system. The database does provide metadata for identifying and classifying records. Safeguards are in place for data input, according to parameters established by the VA.

Information in the database is encrypted both in transit and at rest. Login procedures require the use of PIV cards. Audit trails are used to monitor access, revisions, and other RM activity. Full text searching of records is possible. Using a web browser on a computer that is connected to the AITC intranet, the user navigates to the EAS Registries web site. The servers are covered under the AITC site accreditation.

The web servers are hardened following approved AITC standard security configuration guidelines. Virus protection software is installed on all servers, and updates are performed using an automated process. Security staff monitor the network via intrusion detection.

The Database has Oracle Recovery Manager (RMAN) backup and recovery procedures in place. An Oracle database client, RMAN automates administration of backup strategies and ensures database integrity. Block-level corruption detection is provided during backup and restore. Backup techniques such as parallelization of backup/restore data streams, a backup files retention policy and a detailed history of backup operations are supported.

RMAN handles the underlying maintenance tasks that must be performed before or after any database backup or recovery. It can conduct incremental backups, block media recovery, binary compression, encrypted backups, automated database duplication and cross-platform data conversion. The backup schedule is daily-incremental and weekly-full. In addition, archive log backups are performed three times a day. However, there has been no testing done on the backups or restores to ensure that none of the metadata or timestamps change.

The database supports searches in response to information requests, including FOIA requests, within the live system. Records in the database cannot be deleted and are updated frequently. All information is stored in the live database, and that database is backed up through a manual

process to the facility in Philadelphia. The database has the capability to generate reports demonstrating controls and compliance within the risk management framework.

Environmental Agent Service Registries Databases Records Management Details

IRR and AOR currently have an active schedule that is up to date. The last transfer to NARA was made in August 2021. The next transfer is not due to NARA until 2026. The business owner for these databases is the VA Healthcare Outcomes Military Exposure Office (HOME), and the Office of Information Technology (OIT) does all the technical management of the databases. RM responsibilities are assigned to both federal government staff and contractors at 170 medical centers and 800 outpatient clinics. All contractors and VA employees must sign a Rules of Behavior (ROB). All records retained in the database are permanent, and there have been no issues transferring flat files to NARA so far. Metadata is maintained along with the database. Information in the database is used by the VA only, and not by any other federal agency. Additionally, the database is subject to a yearly audit by the OIG and did receive an ATO from OIT prior to launch.

Findings and Recommendations for Environmental Agent Service Registries Databases

Finding 1: No testing of the backup and restore procedures.

VHA OIT does not test the backup and restore, which can cause issues and create doubts about the record's integrity. If backup and restore choices are not tested, there is a chance that restored data could be tampered with or corrupted.

Recommendation 1: OIT should implement a routine testing program for backup and restore options to ensure the accuracy of electronic records. To guard against any changes or corruption, this testing should include validating the completeness and accuracy of the recovered records and metadata. (36 CFR 1236.10(c))

INSTITUTE OF MUSEUM AND LIBRARY SERVICES

In this report we inspected two databases from the Foundation for Art and Humanities. These were the State Program Report (SPR) Database and Institute of Museum Services (IMS) History database.

The Institute of Museum Services History Database Introduction

The IMS History Database is inactive. When operational, the IMS history file was a computer record of all applications received by IMS and the final actions regarding applications. We were informed by the IMLS ARO that this system is no longer in use and that they were unsure if the records were transferred to NARA. Upon further research with the NARA Electronic Records Processing Branch, no records from this database have been transferred to NARA. The IMS database was decommissioned in 1997 according to the ARO. The ARO stated that the records schedule does not require retention after 10 years. However, according to its records schedule, N1-288-94-001, cutoff should happen at the end of each fiscal year and should be transferred once the records are three years old.[14] Since the database is now inactive, IMLS should have notified NARA to communicate this information.

The State Program Report Database Introduction

The State Program Report (SPR) is a reporting tool used by the freely associated states, the District of Columbia, and the U.S. territories for the IMLS Grants to States Program. This program is the largest source of federal funding support for library services in the U.S. Using a population based formula, funds are distributed among the State Library Administrative Agencies (SLAA) every year and ultimately support around 1,500 projects. The system provides SLAAs the ability to file financial and performance reports It also provides IMLS staff the opportunity to review the data and send back the report for needed edits before it is accepted and made available in the SPR Public View.

Technical Details of the State Program Report Database

The IMLS database management system utilizes SQL Server 2017 Web Edition and is hosted on Amazon Relational Database Services (RDS). The system communicates with the database using .NET technology. Additionally, it is deployed within the AWS GovCloud.

The origin of the system predates all current staff, and it is believed that RM requirements for retention, access, and transfer were not incorporated into the initial system design. Nevertheless, all the entries in the database are considered permanent records. Data can only be entered by authorized users assigned to roles with varying levels of permissions. Multi-factor authentication is used, and access is through a VPN only, which ensures data in transit is encrypted. However, data as whole residing in RDS is not encrypted at rest. This was an informed decision as the SPR data stored in the database is public and data at rest encryption would incur performance/cost overhead. However, user passwords required for authentication are encrypted at rest. Amazon Cloudwatch is used to log and monitor access. IMLS does maintain application and database logs

[14] Institute of Museum Services (IMS) History Database. (n.d.). National Archives. Retrieved February, 2024, from https://www.archives.gov/files/records-mgmt/rcs/schedules/independent-agencies/rg-0288/n1-288-94-001_sf115.pdf.

that will help IMLS staff in tracking activities pertaining to records management, user activity, and cyber security.

Security patches are regularly applied to protect against any threats or vulnerabilities. FISMA 800-53 controls are in place and the system has an authority-to-operate (ATO) that meets 36 CFR guidelines for unauthorized access, disposition, and alteration of records. User rights are based on the principle of least privileged access. RDS automatic backups are performed once daily. The possibility of data loss within a 24-hour window is acknowledged and accepted as a risk. Some of IMLS mission critical systems are part of a COOP Plan, however, SPR is not included. Restoration of the system can be done in a few hours on AWS and daily and weekly snapshots are taken. Information lost over shorter periods of time is considered an acceptable risk.

Amazon cloud reports can be generated to demonstrate system compliance with technical standards, but not specifically with regards to RM. When this system was migrated from on premise to AWS, a data verification exercise was performed and there was no indication of any data loss. To help ensure the continued usability of system records, the version of Excel output by the system is kept up to date.

Records Management Details of the State Program Report Database

IMLS currently has an active schedule for the SPR database. IMLS RM is unsure if the schedule needs updating. The SPR database is used by staff outside of IMLS. State employees have access to the database, and they are governed by assurances and certifications that are signed prior to access. Records were last transferred to NARA in 2013. The next transfer of records is due sometime around 2028. As with their previous transfer, the data will be exported and transferred to NARA in an Excel file format (.xlsx) in accordance with NARA Bulletin 2018-01. There is a public version of this database that is read only. According to the ARO, the system is rarely subject to FOIA requests as information is generally available in the public database. The public version of the database allows users to download and search easily within Excel. As a way to maintain compliance with RM and technical security requirements, each state with access must have their senior official sign documentation of understanding and procedures to have continued access to the system. In addition, state users are frequently vetted by IMLS to have continued access to SPR.

Findings and Recommendations for IMS History and SPR Databases

Finding 1: The IMS History and SPR records schedules may not be up to date.

There seems to be confusion on the status of the records that were a part of this database. Although believed to be inactive, it seems as though the corresponding records that were going in this database are still being produced. Furthermore, the ARO should determine if the schedule for SPR is current.

Recommendation 1.1: IMLS must schedule the records that were once in the IMS History database. (36 CFR Part 1225.22)

Recommendation 1.2: IMLS should determine if the SPR records schedule is up to date. (36 CFR Part 1225.22)

Finding 2: The records produced by the IMS History database have not been transferred to NARA.

Despite the database being inactive, records were still being collected. Since the schedule has not been superseded, the records should still have been transferred to NARA. According to our records, a transfer of records from 1995 to 2020 is overdue.

Recommendation 2.1: IMLS must transfer overdue records to NARA's Electronic Records Branch. (36 CFR 1235.12)

Recommendation 2.2: Since the records have not been transferred and the system is deemed inactive, IMLS may need to investigate if records have been lost and determine if an unauthorized disposition case needs to be opened. (36 CFR Part 1230)

Finding 3: The SPR Database does not have a Requirements Traceability Verification Matrix.

There is no RTVM that maps all test cases to RM requirements, and there is no formal CCB in place for system governance. There is, however, a technical lead who discusses system issues tracked in Jira on a weekly basis.

Recommendation 3.1: IMLS should create an RTVM for SPR to manage and map all test cases. (1236.2 - Quality Assurance)

Recommendation 3.2: IMLS should Implement a CCB for system governance beyond the current Jira tracking. (1236.2 - Quality Assurance)

Finding 4: Data in SPR is not encrypted at rest.

During the interview, it was stated that RDS data is not encrypted at rest and only encrypted in transit. (36 CFR 1236.34)

Recommendation 4: IMLS should work to understand the Amazon RDS and see if data can both be encrypted in transit and at rest to ensure greater security and oversight of the records.

UNITED STATES PAROLE COMMISSION

We inspected two databases from the United States Parole Commission (USPC): the Decision Reporting and Monitoring (DRAM) System and the Parole Decision Making System.

United States Parole Commission Databases Introduction

The Parole Decision Making System was used to house individual paroling considerations (including hearings, appeals, reopenings, and reviews on the record). Each record contains approximately forty items, including sentence parameters and the results of the paroling consideration (NC1-438-85-02).

DRAM was a database that maintained records of each parole hearing from 1972 until 2018; and it monitors the Commission's parole decisions to ensure compliance with pertinent regulations and guidelines (N1-438-00-001).

United States Parole Commission Databases Technical Details

The Parole Decision Making System was a hybrid paper and electronic system. The paper from Parole Decision Making System was scanned as an image into DRAM. Furthermore, the DRAM database is now considered obsolete as of December 2018. The system is still available for read-only access on the USPC's SQL server.

Not much technical information was known about the Parole Decision Making System or DRAM due to the age of the systems and the turnover in staff at USPC. We know that each record in the Parole Decision Making System is identified by the Bureau of Prisons register number. Likewise, not much technical information was known about DRAM.

DRAM and essentially the Parole Decision Making System have been absorbed by the USPC's Offender Management System (OMS). DRAM was partially migrated into OMS. The DRAM information was migrated into the new database, but the parole decision data was not. Additionally, of the information migrated, only active record information was migrated. If the record was closed at time of migration, then the record can only be found in DRAM on the SQL server. OMS was created to adhere to the FISMA Act of 2014[15]. OMS is run on Entellitrak (ENTK). ENTK is at[16]. OMS is a centralized system used by many sub-agencies of the United States Department of Justice (DOJ). Centralization allows for better maintenance, monitoring and security.

More information is present about the active but unscheduled ENTK Offender System. OMS has daily incremental backups of the data within it. The database is currently going through a migration. The ENTK software is being updated. This update will require a data migration. The data will be verified and validated after the migration through testing and reviewing of the logs

[15] Audit of the Criminal Division's Entellitrak System Pursuant to the Federal Information Security Modernization Act of 2014 Fiscal Year 2018. (2017, November 9). Oversight.gov. Retrieved February, 2024, from https://www.oversight.gov/sites/default/files/oig-reports/a1928.pdf.

[16] *Application Platform*. (n.d.). Tyler Technologies. Retrieved February, 2024, from https://www.tylertech.com/products/application-platform.

for any potential errors. USPC will perform a detailed comparison with the data that was migrated with the existing data stored on the original database. USPC has a restoration process plan in case records are damaged during migration. This same restoration plan is in place when there is not a migration plan. The restoration plan is a part of their data recovery plan, where daily backups of the system can be restored back to the last successful operational timeline. USPC uses audit logs and monitoring systems in place to track access and changes to the data during migration. Additionally, they incorporate validation checks to ensure data integrity at various stages of migration, including source data, transformation, and destination storage.

United States Parole Commission Databases Records Management Details

There are two separate approved record control schedules for these databases, however, we discovered during the interview that the Parole Decision Making System was absorbed by DRAM. Both DRAM and the Parole Decision Making System have active record schedules despite both being obsolete and inactive. DRAM was previously named the Parole Decision History (PDH) System. There is still an active schedule for PDH as late as 2021. A superseded notice was attached to the schedule but still states that DRAM is active (NC1-438-85-02).

The Offender System currently is not scheduled. The RM team at DOJ is no longer confident that the records in OMS are permanent. There is a conventional thought within the RM team that records should be considered temporary. At the time of the interviews, they were still considering all options. Furthermore, some were concerned that the records in DRAM and the Parole Decision Making System should be temporary as well. Due to the age of the schedules for DRAM and the Parole Decision Making System, the staff that worked on scheduling these records are no longer at the agency and there is insufficient documentation on the DOJ and USPC side to use for reference.

Records from the Parole Decision Making System and DRAM were transferred to NARA in 2013. NARA has not taken legal custody of any Parole Decision Making System or DRAM records since 2013. DOJ and USPC believes that when this transfer occurred 2013, all records from the Parole Decision Making System were exported and provided to NARA, as well as many records from the DRAM system. According to DOJ and USPC, NARA should only be missing records from the DRAM system from 2013-2018.

The records are currently sitting on a SQL Server on-premises at a DOJ facility. There is currently no records management policy for the current DRAM system. According to IT staff during the interview, only active systems at DOJ have a RIMCert. Due to the age of the DRAM system, the current RM and IT staff at DOJ and USPC were not able to provide much technical information about the system or its predecessor.

Findings and Recommendations for United States Parole Commission Databases

Finding 1: Only Select Data was Migrated to the New Database.

Only active data at the time of the migration was migrated from DRAM to OMS. It is unclear whether the data in the new database matches the fields of the older database.

Recommendation 1: USPC needs to locate the data not migrated to OMS and manage it in preparation for a transfer to NARA. USPC could work to migrate the data to OMS and keep the data hidden from the user interface of the system. (36 CFR 1236.10) (36 CFR 1236.14)

Finding 2: Records Schedules are Outdated or Need to be Created.

The records schedules for the Parole Decision Making System and DRAM are out of date since the system is technologically obsolete. There is no schedule for their successor, the UPSC Offender System. The records need to have a determination of their status. Are the records permanent or temporary?

Recommendation 2.1: The USPC needs to determine if the records in the Parole Decision Making System, DRAM, and OMS are permanent or temporary. (36 CFR 1225.14(c)) (36 CFR 1225.16(a))

Recommendation 2.2: USPC needs to formally notify NARA that both the schedule for the Parole Decision Making System and the DRAM system need to be updated as inactive. (36 CFR 1225.10) (36 CFR 1225.22)

Recommendation 2.3: The USPC needs to create a new schedule for the records in OMS. (36 CFR Part 1225)

Finding 3: If the Records are Considered Permanent, the Records are Overdue for Transfer.

The current schedule is written as though the records are permanent in the Parole Decision Making System and DRAM. There has never been a transfer of these records to NARA.

Recommendation 3: If the records are determined to be permanent, the records of the Parole Decision Making System and DRAM need to be transferred to NARA in accordance with the schedule and the NARA Transfer Guidance. (36 CFR Part 1235 Subpart B) (36 CFR 1235.50)

Finding 4: There was no RIMCert for DRAM. RIMCert for OMS is in progress.

Although the DRAM system did not have a RIMCert, the DOJ's Records Management Office and USPC are currently working on the RIMCert for OMS. USPC submitted a RIMCert for the system in February 2024, and the DOJ's Records Management Office has been coordinating with them to implement.

Recommendation 4: To protect the integrity, security, and reliability of records, and to prevent further technological obsolescence records, USPC needs to continue to work with the DOJ's Records Management Office to implement the RIMCert to OMS. . (36 CFR 1236.10) (36 CFR 1236.14)

APPENDIX

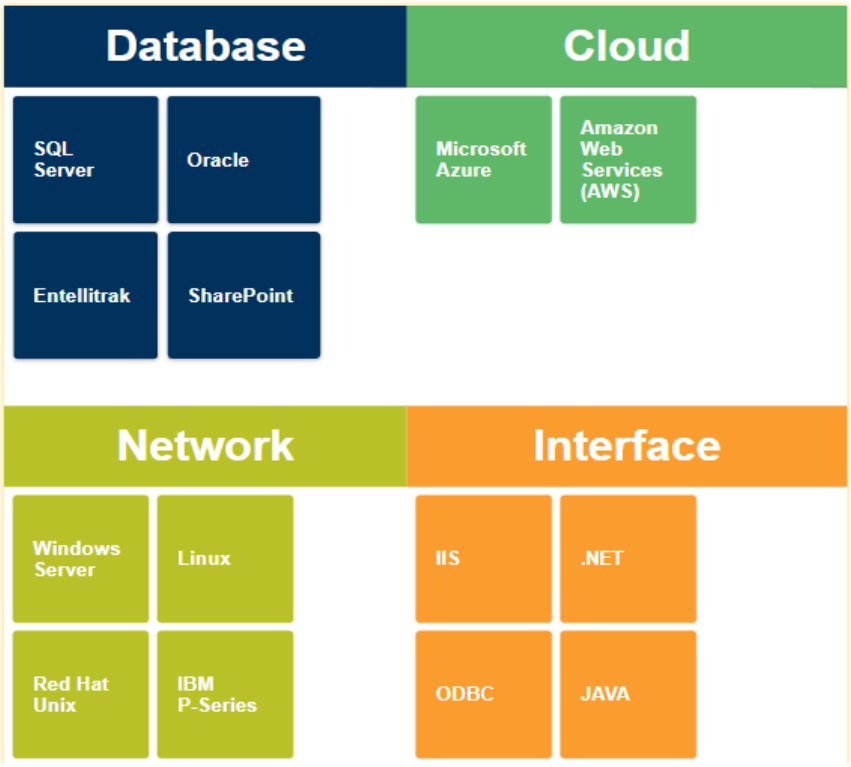
METHODOLOGY

As part of the function of the systems analysis of the databases studied in this report, we not only seek to ensure that proper records management governance is taking place, but also that proper information technology system management is happening. To that end, we categorized our questions into the following high-level categories:

- Records Management
- System Design and Implementation
- Operations and Maintenance
- System Testing and Configuration Management
- Policy and Oversight

TECHNICAL APPROACH

Due to the sheer number of databases that were inspected the technical observations were vast. Each respective database, even within agencies, used different database platforms, architecture environments, and interfaces. These ranged from:



On top of the various flavors of database technology each database function and purpose provided challenges to draw a common technical theme(s). The report is focused on overall observations and high-level technical findings, with an emphasis on RM and best practices that we observed through discussions and documentation.

For the technical aspects we focused on our methodology stated above and geared the questions according to those parameters. This approach allowed us to ask the same questions and request the same documents for each database. For each database inspected you will find the report has an introduction which provides basic understanding of the function and use of the database, This is followed by a technical detail section which provides a technical overview based on interview questions and submitted documentations. The last section is findings and recommendations which provides any observations, findings or suggested actions.

A technical agnostic approach to the inspection was also a way to provide observations without judgment of strengths and weaknesses of the system platforms rather allowing the inspection to focus on record integrity and eventual transfer to NARA.

AGENCY DATABASE STATISTICS

Database Name	Updated Record Schedule	Database Size	Technical Details
Decision Reporting and Monitoring (DRAM) System	No	Unknown	Unknown
Parole Decision Making System	No	Unknown	Unknown
Regional Partnership Grant Evaluation Data System	Yes	Not provided	Microsoft Azure Government Cloud Platform leveraging Platform-as-a-Service (PaaS)
Office on Trafficking in Persons (OTIP) (Shepherd 1.0)	Yes	Not provided	Amazon Relational Database Service Structured Query Language (SQL)
State Program Report (SPR) Database	Unsure	803 MB Approx 2 million records	Amazon Relational Database Service Structured Query Language (SQL) Server 2017
IMS History Database	Unsure	Not provided	Unknown
Ionizing Radiation Registry (IRR) Records	Yes	~ 17 GB	Runs on Oracle 19
Agent Orange Registry (AOR) Records	Yes	Not provided	Runs on Oracle 19c
Burial Operations Support System (BOSS) and the Automated Monument System (AMAS)	Yes	Approx 10 million records; ~10TB	Amazon Web Services, Oracle Database, Red Hat Unix, IBM P-Series, Weblogic
Bomb Arson Tracking System (BATS) Database	No	2-4 TB	Web based built on .NET framework
Firearms Tracing System (FTS)	Yes	Not provided	Oracle Database and a Windows application

GLOSSARY

ACF	Administration For Children and Families
AITC	Austin Information Technology Center
AMAS	Automated Monument Application System
AOR	Agent Orange Registry
ArcGIS	A Geographical Information System
ARO	Agency Records Officer
ATF	The Bureau of Alcohol, Tobacco and Firearms and Explosives
ATIMS	Anti-Trafficking Information Management System
ATO	Authority to Operate
AWS	Amazon Web Services
BATS	Bomb Arson Tracking System
BLOB	Binary Large Object
BOSS	The Burial Operations Support System
BOSS-E	Burial Operations Support System Enterprise
CCB	Change Control Board
CFR	Code of Federal Regulations
COOP	Continuity of Operations Plan
COTS	Commercial Off the Shelf
DFuze	The original tracking system used by ATF that was superseded with BATS
DOJ	Department of Justice
DRAM	Decision Reporting and Monitoring System
EA	Enterprise Architecture
EAS/R	Environmental Agent Service Registries
ENTK	Entellitrak - A low-code application development platform for case management
ERD	Entity Relationship Diagram
Esri	Environmental Systems Research Institute
FBI	Federal Bureau of Investigation
Feith	A commercial off the shelf software product used for the storage and management of images
FLS	Firearms Licensing System
FOIA	Freedom of Information Act
FTS	Firearms Tracking System
HDS	Hazardous Devices School
HHS	Department of Health and Human Services
IMS	Institute of Museum Services
IRR	Ionizing Radiation Registry
KCL	Kiosk - Nationwide Gravesite Locator
MOU	Memorandum of Understanding
MPS	Memorial Program Service

NARA	National Archives and Records Administration
NCA	National Cemetery Administration
NGL	National Gravesite Locator
NTC	National Tracing Center
OIT	Office of Information Technology
OTIP	Office on Trafficking in Persons
PaaS	Platform-as-a-Service
PDH	Parole Decision History
PIV	Personal Identity Verification
RDS	Amazon Relational Database Services
RIM	Records and Information Management
RIMCert	Records and Information Management Certification
RM	Records Management
RMAN	Recovery Manager
ROB	Rules of Behavior
RPG-EDS	Regional Partnership Grants Evaluation Data System
RTVM	Requirements Traceability Verification Matrix
SAORM	Senior Agency Official for Records Management
SDLC	System Development Life Cycle
SIARD	Software Independent Archival of Relational Databases
SLAA	State Library Administrative Agencies
Splunk	Security Auditing Software
SPR	State Program Report
SQL	Structured Query Language
SSP	System Security and Privacy Plan
UD	Unauthorized Disposition
USPC	United States Parole Commission
XTS	Explosives Tracking System

REFERENCES

§ 1235.12 When must agencies transfer records to the National Archives of the United States? (2009, October 2). eCFR. Retrieved February 1, 2024, from https://www.ecfr.gov/current/title-36/section-1235.12.

Appendix A: Tables of File Formats. (2023, September 8). National Archives. Retrieved February 12, 2024, from https://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html
Application Platform. (n.d.). Tyler Technologies. Retrieved February, 2024, from https://www.tylertech.com/products/application-platform.

Audit of the Criminal Division's Entellitrak System Pursuant to the Federal Information Security Modernization Act of 2014 Fiscal Year 2018. (2017, November 9). Oversight.gov. Retrieved February, 2024, from https://www.oversight.gov/sites/default/files/oig-reports/a1928.pdf.

Bulletin 2015-04. (2015, September 15). National Archives |. Retrieved January 24, 2024, from https://www.archives.gov/records-mgmt/bulletins/2015/2015-04.html.

Firearms Tracing System (FTS). (n.d.). National Archives. Retrieved February 12, 2024, from https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0436/n1-436-96-004_sf115.pdf.

Institute of Museum Services (IMS) History Database. (n.d.). National Archives. Retrieved February, 2024, from https://www.archives.gov/files/records-mgmt/rcs/schedules/independent-agencies/rg-0288/n1-288-94-001_sf115.pdf.

INTERNATIONAL STANDARD ISO 15489-1. (2016, April 15). iTeh Standards. Retrieved February 8, 2024, from https://cdn.standards.iteh.ai/samples/62542/fe383f4fe10448d5b22ce628b1542ed6/ISO-15489-1-2016.pdf.

NARA's Unauthorized Disposition Reporting Requirements. (2017, November). National Archives. Retrieved February, 2024, from https://www.archives.gov/files/records%20mgmt/resources/ud-submission-instructions.pdf.

NARA Transfer Guidance. (2023, September 8). National Archives. Retrieved February 5, 2024, from https://www.archives.gov/records-mgmt/policy/transfer-guidance.html.

Office of Compliance Operations: Firearms Licensing System (FLS). (n.d.). National Archives. Retrieved February 1, 2024, from https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0436/n1-436-94-001_sf115.pdf.

Records Management by the Archivist of the United States (44 U.S.C. Chapter 29). (2022, March 3). National Archives. Retrieved January 12, 2024, from https://www.archives.gov/about/laws/records-management.html.

SIARD Format Specification. (2021, August 31). SIARD. Retrieved February, 2024, from https://siard.dilcis.eu/SIARD%202.2/SIARD%202.2.pdf.

36 CFR 1225.22 -- When must agencies reschedule or review their records schedules? (2009). eCFR. Retrieved February 2, 2024, from https://www.ecfr.gov/current/title-36/chapter-XII/subchapter-B/part-1225/section-1225.22.

36 CFR Part 1235 -- Transfer of Records to the National Archives of the United States. (2009). eCFR. Retrieved February 1, 2024, from https://www.ecfr.gov/current/title-36/part-1235#p-1235.12(b).

Unauthorized Disposition of Federal Records | National Archives. (2016, October). National Archives. Retrieved February 12, 2024, from https://www.archives.gov/records-mgmt/resources/unauthorizeddispositionoffederalrecords.

AUTHORITIES

- 44 U.S.C. Chapter 29
- 36 CFR 1235.12
- 36 CFR 1235.12
- 36 CFR Part 1225.22
- 36 CFR 1223.14
- 36 CFR Part 1230
- 36 CFR 1236.14
- 36 CFR 1236.10
- 36 CFR 1236.2
- 36 CFR 1236.34
- 36 CFR 1225.16
- 36 CFR 1225
- 36 CFR 1225.10
- 36 CFR Part 1235 Subpart B
- 36 CFR 1235.50

OTHER GUIDANCE

- NARA Universal Electronic Records Management (UERM) Requirements - https://www.archives.gov/records-mgmt/policy/universalermrequirements
- NARA Bulletins - https://www.archives.gov/records-mgmt/bulletins
    - *Format Guidance for the Transfer of Permanent Electronic Records* (NARA Bulletin 2014-04) - https://www.archives.gov/records-mgmt/bulletins/2014/2014-04.html
    - *Agency Records Management Training Requirements (*NARA Bulletin 2017-01) - https://www.archives.gov/records-mgmt/bulletins/2017/2017-01-html
    - *Updating NARA Bulletin 2014-04, Format Guidance for the Transfer of Permanent Electronic Records* (NARA Bulletin 2018-01) -

https://www.archives.gov/records-mgmt/bulletins/2018/2018-01

- Federal Records Management, Unauthorized Disposition of Federal Records - https://www.archives.gov/records-mgmt/resources/unauthorizeddispositionoffederalrecords
- Frequently Asked Questions (FAQs) About Transferring Permanent Electronic Records to NARA - https://www.archives.gov/records-mgmt/faqs/transfer-erec
- NARA *Unauthorized Disposition Reporting Requirements* - https://www.archives.gov/files/records-mgmt/resources/ud-submission-instructions.pdf
- U.S. Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* - https://www.gao.gov/assets/670/665712.pdf
- Office of Management and Budget (OMB) Memorandum M-16-17 and OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* - https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

STATUTES AND REGULATIONS

36 CFR Chapter XII, Subchapter B, specifies policies for Federal agencies' records management programs relating to proper records creation and maintenance, adequate documentation, and records disposition. The regulations in this Subchapter implement the provisions of 44 U.S.C. Chapters 21, 29, 31, and 33. NARA provides additional policy and guidance to agencies at its records management website - http://www.archives.gov/records-mgmt/.

At a high level, agency heads are responsible for ensuring several things, including:

- The adequate and proper documentation of agency activities (44 U.S.C. 3101);
- A program of management to ensure effective controls over the creation, maintenance, and use of records in the conduct of their current business (44 U.S.C. 3102(1)); and
- Compliance with NARA guidance and regulations, and compliance with other sections of the Federal Records Act that give NARA authority to promulgate guidance, regulations, and records disposition authority to Federal agencies (44 U.S.C. 3102(2) and (3).