

Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)



Privacy Impact Assessment for Digital Signage System (e-Boards)

Issued by:

[Varun Bisht, Senior Component Official for Privacy]

Approved by: Brian A. Young
Deputy Director (Acting)
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: December 10, 2024

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) uses several methods to communicate information in a clear, concise, and easily digestible manner internally to all agency personnel. The three primary methods are Daily Broadcast¹ email messages, ATF Connect Portal² website community announcements, and the e-Boards Digital Signage system. The eBoards Digital Signage system consists of content management and production software, as well as the electronic boards (herein referred to as “e-Boards”) that display the finished content for ATF communications purposes.

The e-Boards solution is designed to provide information to ATF employees and visitors on centrally located high definition (HD) display monitors at ATF Headquarters. The main advantage of e-Boards is that they are dynamic, eye-catching, easily updatable, engaging, and allow notification to a large community without having to be at or on a computer.

Content submitted for display is sent to the ATF’s Digital Media Division (DMD) for review and editing. It is then posted to the e-Boards, e.g., as a reminder of an event or to highlight the importance of announcements such as event invites, mandatory trainings, monthly campaigns, and explanations of new procedures or policies. There are four content managers in DMD with access to the application and hardware, who are responsible for the creating, publishing, and approving all announcements displayed with e-Boards.

ATF prepared a Privacy Impact Assessment for e-Boards Digital Signage system because the system displays information, such as pictures and will include names of employees, contractors, and detailees in open areas within ATF’s Headquarters compound (ATF Headquarters) which is accessible to ATF employees, contractors, and detailees, as well as authorized visitors.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component’s purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify

¹ Daily Broadcast is a daily ATF-wide email containing announcements and notices of interest to the ATF community (job announcements, promotions, birth and obituary) that is sent to all ATF personnel (federal employees, and contractors) with an official ATF email address.

² ATF Connect Portal is the official ATF website, consisting of an internal portal for employees, an external publicly available site, and a section for community notices and announcements which are accessible to both ATF and public audiences.

previously unknown areas of concern or patterns.

ATF e-Boards Digital Signage consists of content management software, production software, and display hardware, including the electronic displays, hard drives with network connection devices, and micro-SD memory cards (collectively, “e-Boards”). BrightAuthor is the content management application developed by BrightSign³ LLC that provides a user-friendly interface that makes creating, publishing presentations, and managing the closed network of e-Boards simple and dependable. The eight displays, that are not interactive touchscreen displays, are strategically placed in the atrium and at the elevator bay on each floor of ATF Headquarters, which are central locations for community announcements.

The content delivered to the e-Boards reflects information that is disseminated via the ATF Daily Broadcast (DB) Announcement emails and ATF Connect Portal, such as fitness and wellness classes, volunteer opportunities, and press releases on ATF missions or events. “People-related” announcements, such as births, promotions, and retirement announcements that identify specific individuals are prohibited from display. The DMD content managers manually copy and edit content from the DB, create an image to accompany the content, and then save the file onto an ATF SharePoint drive and “publish” that image as a slide via BrightAuthor. The slides are saved under the title of the announcement and are then placed into the rotation queue and displayed on the e-Boards.

ATF community members who submit a request for content to be posted must adhere to the policy outlined in the ATF Public Information Officers (PIO) Guide, which provides instructions and guidance for what can be displayed. In addition to ATF-centric information, ATF subscribes to three publicly available information feeds, which are selected for their content and usefulness for ATF personnel. These feeds report statuses (arrivals, departures, and delays) for Washington Metropolitan Area Transit Authority Metro trains, current Office of Personnel Management (OPM) operating status for Federal Agencies in the DC metro area (building closures, events), and weather alerts. The e-Boards display information 24 hours every day at the discretion of ATF’s Office of Public and Governmental Affairs (PGA).

Separately, there are two interactive digital touch-screen e-Boards located next to the Fallen Agents Memorial Wall, which is located within the ATF Headquarters compound and is accessible to those with authorized access to the compound, including ATF staff and approved visitors. DMD employees update these two e-Boards as needed, by replacing a Micro Secure Digital (microSD) card that stores and transfers data and includes the necessary updated information that will be displayed. The only content displayed on the two e-Boards located next to the Fallen Agents Memorial Wall is collected from ATF’s Fallen Agents webpage, which is located on ATF’s public-facing website. Users can browse through the names, photos, and biographies of fallen ATF agents, or watch a video about the memorial.

2.2 *Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)*

³ BrightSign LLC is the vendor who builds, maintains, and sells both the hardware and the software for Digital Signage. The vendor does not have any access to stored ATF data.

Authority		Citation/Reference
X	Statute	5 U.S.C. § 301 - Government Organizations and Employees 28 U.S.C. § 599A - Bureau of Alcohol, Tobacco, Firearms, and Explosives
	Executive Order	
X	Federal Regulation	28 CFR Subpart W - Bureau of Alcohol, Tobacco, Firearms, and Explosives
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 *Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Name	X	A	Names of ATF employees, contractors, and detailees who are the subject or point of contact listed in an announcement.
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			

Department of Justice Privacy Impact Assessment

ATF/e-Boards

Page 4

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Passport number			
Mother's maiden name			
Unique Personal Identification Number (UPIN)			
Vehicle identifiers			
Personal address			
Personal e-mail address			
Personal phone number			
Business address			
Business e-mail address	X	A	Email address for ATF employees, contractors, and detailees who are the point of contact listed in an announcement.
Business phone number	X	A	Office phone numbers for ATF employees, contractors, and detailees may be listed, as needed.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			

Department of Justice Privacy Impact Assessment

ATF/e-Boards

Page 5

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
<i>Biometric data:</i>			
- Photographs or photographic identifiers	X	A & B	Photos may be displayed in relation to an announcement.
- Video containing biometric data	X	A & B	Videos (without audio) may be displayed in relation to an announcement; software does not have facial recognition capabilities
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			
- Voice recording/signatures			
- Scars, marks, tattoos	X	A & B	Displayed photos may include scars, marks, or tattoos.
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify)			
<i>System admin/audit data:</i>			
- User ID			
- User passwords/codes			
- IP address	X	A	IP address of four DMD content managers responsible for managing the e-Boards system.
- Date/time of access			
- Queries run			
- Content of files accessed/reviewed			
- Contents of files			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A & B	Announcements may contain information or PII that may be unanticipated at the time of this PIA.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Requests for information to be posted are sent via email. All content must be approved through ATF's chain of command (through both the office making the request and the DMD manager) before it can be posted. When ATF community members submit content (only ATF personnel can submit content though, as indicated, some content may come from other DOJ components), the method of delivery can be specifically requested.					

Non-government sources:					
Members of the public		Public media, Internet	X	Private sector	
Commercial data brokers					
Other (specify): Weather information is pulled from the company Creating Margin Technology Group. Real-time metro station updates are pulled from Washington Metropolitan Area Transit Authority (WMATA). ⁴					

⁴ Washington Metropolitan Area Transit Authority (WMATA) provides publicly available, free of charge subscriptions for mass transport advisories and alerts.

Section 4: Information Sharing

4.1 *Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.*

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Within the Component	X			Information is displayed throughout the agency on the e-Boards located at the elevator doors, in the atrium, and in the breezeway of ATF Headquarters. Requests for announcements are made to the content managers and approved by the appropriate department chief.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	X			Individuals who are within the viewing area of the e-Boards will have access to the information displayed. During public events, such as an open house at the ATF Headquarters, the e-Boards are cleared out on the first floor and a full screen poster for the day is displayed. Once the event is over, the e-Boards go back to the normal announcement template.

4.2 *If the information will be released to the public for “[Open Data](#)” purposes, e.g., on data.gov*

(a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

e-Boards do not have data or statistical information that would be released to the “Open Data” site (www.data.gov).

Section 5: Notice, Consent, Access, and Amendment

- 5.1** *What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.*

The e-Boards system does not create a new System of Records. The information selected for the announcements is not maintained or archived in the e-Boards application, and therefore, it is not possible to search for individual information based on personal identifier

In the case where a supervisor may wish to highlight an individual’s professional accomplishment, the ATF employee, contractor, or detailee can notify their supervisor they wish to opt out of this kind of display of information in e-Boards or elsewhere.

- 5.2** *What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.*

In the case where a supervisor may wish to highlight an individual’s professional accomplishment, the ATF employee, contractor, and detailee can notify their supervisor they wish to opt out of this kind of display of information in e-Boards or elsewhere. Individual employees are part of the submission process and may contact DMD and request removal of their information at any time before or after an item is displayed, and DMD will review the request against DMD policy and determine whether to remove the content.

- 5.3** *What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.*

Members of the public, as well as individuals to whom the information pertains, may submit a FOIA or Privacy Act request for information displayed using e-Boards.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO): Granted: May 1, 2024 Expires: May 1, 2027 If an ATO has not been completed, but is underway, provide status or expected completion date: Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation: One POAM is currently open to implement automation of syncing system logs.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: e-Boards has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, the system has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook. The system operates within the boundary of ATF's primary infrastructure environment, where it is subject to full system monitoring and audit in accordance with ATF and Department guidelines. All system documentation supporting these activities are maintained within the Department's system of record, Joint Cybersecurity Assessment and Management (JCAM) tool.
X	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted: Currently, authorized system administrators can manually access ad hoc security logs, as needed, as part of the security and privacy process while ATF is in the process of implementing an automated process.
	Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy. Currently, contractors do not have access to e-Boards or the underlying system.
X	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel

on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:

All e-Boards users are subject to organizational and Department annual computer security awareness and privacy specific training that includes sign off and acknowledgment of the DOJ General and Privileged Rules of Behavior. All employees of ATF are required to complete annual privacy and cyber security online training through the Justice Talent Management System (JTMS). There is not additional training specific to this system.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

e-Boards has four approved data managers with access to the application that manually copy and edit content, create an image to accompany the content, and then save and “publish” that image via the Bright Author so that it displays on the e-Boards, in accordance with the ATF’s PIO Guide. Access to the microSD card readers in the e-Boards are physically locked, and the RSS feed is managed through the software so only the four ATF employees approved as content managers may select and authorize which RSS feeds to display.

The e-Boards are located within ATF’s Headquarters Access to the ATF Headquarters is restricted to ATF employees, contractors, detailees, and authorized guests.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Announcements displayed by e-Boards are transitory and have short-term or immediate value for the ATF community and stakeholders. The information displayed in e-Boards are handled according to ATF Record Control Schedule Order 1340.7. Item # 1006 (transitory records), which states that they are destroyed when there is no further business use. The NARA retention schedule is DAA-GRS-2022-0009-0001, Item GRS 5.2, 010.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as “records” maintained in a “system of records,” as defined in the Privacy Act of 1974, as amended).

 X No. Yes.

7.2 *Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:*

The e-Boards system does not create a new System of Records. The information selected for the announcements is not maintained or archived in the e-Boards application, and therefore, it is not possible to search for individual information based on personal identifier. DMD design/edit the content in either Adobe or Microsoft products. The content is then pushed to the eBoards via the Brightsign software. Upon expiration, the content is deleted.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- *Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),*
- *Sources of the information,*
- *Specific uses or sharing,*
- *Privacy notices to individuals, and*
- *Decisions concerning security and privacy administrative, technical and physical controls over the information.*

ATF uses e-Boards as an electronic bulletin board for presenting notifications to the ATF community. The privacy risks associated with information collected for use are primarily related to the loss of confidentiality and integrity of the information displayed on e-Boards and access by unauthorized entities to personal data.

ATF uses standard administrative, technical, and physical safeguards to protect the information displayed in e-Boards from misuse and unauthorized access. The e-Boards are located within ATF Headquarters, which prevents unauthorized physical access by the general public through the use of security guards, sign-in logs, security cameras, and access badge control. Further, appropriate network security controls help protect against risks identified in the security risk assessment, including but not limited to, security controls for account management, access controls, access privileges, authentication, least privilege, account restrictions, account monitoring and control, authenticator management, audit reviews, analysis, and reporting. e-Boards resides on and inherits most of the security controls from ATF's General Support System. The software used for eBoards is not cloud based and has to have a copy downloaded on the local drive of the four approved user computers.

e-Boards is approved for and installed on the computers of four users, all of whom are government

employees and must use their ATF-issued personal identity verification (PIV)⁵ card to access their laptop where the software is installed. The security control of least privilege ensures that there is a clear separation of duties to prevent anyone outside the DMD having access to the system.

To prevent the release of personal information, all announcements will be reviewed for possible privacy concerns prior to submission to the DMD by respective program offices chain of command requesting the announcement. Content delivered to the e-Boards mirrors information that is also disseminated via the ATF Daily Broadcast Announcement, but excludes people related announcements, (e.g., births, deaths, promotions). The individuals reviewing requests to share announcements consider guidance identified in the ATF PIO Guide when authorizing the display of information.

The information selected for the announcements is not stored or archived in the e-Boards application, and therefore, it is not possible to search for individual information based on any element of PII. Upon expiration of the announcement, the content is deleted. This also avoids the over collection of data and possible retention conflicts with the ATF records control schedule. The DMD responsibility is to facilitate the temporary display of information, the retention of this data remains with the submitting management.

⁵ A PIV card is a physical artifact (e.g., identity card, “smart” card) issued to an applicant by an issuer that contains stored identity markers or credentials (e.g., a photograph, cryptographic keys, digitized fingerprint representations) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). See: https://csrc.nist.gov/glossary/term/piv_card.