



# Bomb Arson Tracking System



**\*\* To avoid delays please complete ALL fields \*\***

## Information Access Request Form

User's Information			FAX NUMBER
Name - (Last, First, M.I.)		Position/Title	866-927-4570
Date of Birth	Mother's Maiden Name	SSN (last 4 digits)	Telephone Number
Official Email Address		User's Signature & Date	
Bomb Squad Information (if applicable)			
Official Bomb Squad Number		Expiration Date of HDS Certification	
User's Access Role (check one)			
Local Administrator (maintains agency's accounts)	<input type="checkbox"/> Check Box	Local User	<input type="checkbox"/> Check Box
Agency Information			
Agency Name (This is how your agency name will appear on your reports)			
Address (City, State, Zip)			
Agency ORI Number			
Supervisor Information			
Print Supervisor's Name		Supervisor's Telephone #	
Supervisor's Official E-Mail Address		Supervisor's Signature & Date	
ATF Official Use Only			
ATF System Administrator	Signature	Date Approved	
Comments or additional information			

SIGN HERE

User Sign

SIGN HERE

Mgr Sign

**\*\*If You Are an Agency User, This Form Must Also Be Signed By Your Agency's Designated Account Manager\*\***

**\*\*If You Are an Agency User, This Form Must Also Be Signed By Your Agency's Designated Account Manager\*\***

### Privacy Act Statement

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

**\*\* AVOID DELAYS - USE THE APPLICATION CHECKLIST \*\***  
(see second page)



## Bomb Arson Tracking System (BATS)


### Application Checklist



This checklist provides a self-review process to complete the application **and** avoid delays.  
(This checklist is a guide and not a replacement for the application instructions provided by the USBDC).


- **NEW Agency Account (agency does *not* have a current BATS account)**

#### 1) Agency Request Letter:

- On Official Agency Letterhead;
- Contains ***All*** Information in the Sample Letter Provided by the USBDC  
(required fields in request letter are highlighted by [red] brackets);
- Identifies the Account Manager; and 
- Signed by Agency Head or other Designee

**\*\*Note:** Please reference the e-mail response to your initial BATS application for downloading the request letter.

#### 2) Information Access Request Form (for each new user)

- All*** Sections Completed;
- User's Signature; and 
- Account Manager's Signature

#### 3) Rules of Behavior & User Agreement Form (for each new user)

- User's Signature on last page\*\*; and 
- Account Manager Signature on last page\*\*

**\*\*Note:** Remember to review all pages of the user agreement before signing.

- **EXISTING Agency Account (adding new users to agency's BATS account)**

#### 1) Information Access Request Form (for each new user)

- All*** sections completed;
- User's Signature; and
- Account Manager's Signature

#### 2) Rules of Behavior & User Agreement Form (for each new user)

- User's Signature on last page\*\*; and 
- Account Manager Signature on last page\*\*

**\*\*Note:** Remember to review all pages of the user agreement before signing.

**\*\* Fax All Forms to the USBDC @ 866-927-4570, attn: BATS Unit \*\***



## **Bomb Arson Tracking System (BATS)** **Rules of Behavior & User Agreement Form**



### **Introduction:**

Crimes involving explosives and arson are among the most devastating incidents confronting our society. They destroy property, endanger and disrupt lives, and place an ever-increasing economic burden upon our nation's citizens.

BATS, which was developed exclusively by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), serves as the national repository for information pertaining to bombing, explosives, and arson-related incidents, as mandated by Federal law. BATS includes a functionality that supports the use of the program as a case management system, allowing investigators to build their investigation, while maintaining operational security. ***Each agency is responsible for administering their own BATS account.***

### **Purpose:**

This agreement outlines the acceptable uses of BATS. This user agreement form must be signed before access to BATS is granted. ***A letter requesting access from the user's agency head or designee on official agency letterhead must accompany or precede this user agreement.*** Such letter must identify the agency's designated BATS account manager and other information required by ATF's U.S. Bomb Data Center (USBDC).

### **Authority:**

This agreement is established pursuant to the authority of the participants to engage in activities related to the investigation and suppression of crimes involving fire and the suspected criminal misuse of explosives.

### **References:**

- 18 U.S.C. Chapter 40, authorizes the Attorney General to investigate violations of Federal explosives and arson laws. This authority has been delegated to ATF pursuant to 28 C.F.R. 0.130.
- Public Law 104-208, Omnibus Consolidated Appropriations Act of 1997, authorizes the Attorney General to establish a national repository of information on incidents involving arson and the suspected criminal misuse of explosives.
- Public Law 100-235, Computer Security Act of 1987, requires agencies to identify sensitive systems, conduct security training, and develop computer security plans.
- OMB Circular A-130, Appen III, requires that federal agencies establish security programs containing specified elements.
- ATF H 7250.1 Automated Information System Security Program

### **Background:**

BATS provides simplified case tracking, statistics, trending, and resource management of investigatory elements and administrative tasks related to the mission. Law enforcement and other public safety agencies can use the data to pursue their cases for investigation and prosecution. Data can also be aggregated to determine trends, movement, and possible links that would not be possible from the state and local level.

The BATS program is intended to provide explosive ordnance disposal personnel, fire investigators, and post-blast investigators from law enforcement & other public safety agencies with real-time incident based information within a secure environment. To accomplish this requirement, it is necessary that BATS contain Sensitive But Unclassified (SBU) law enforcement sensitive (LES) data. As a general rule, LES information may be shared with anyone in the law enforcement community who has the right to know and need to know the information. It is critical that such data be properly handled to ensure effective law enforcement operations, officer safety, and the privacy of individuals. ***The lawful and proper use of BATS by its users is mandatory.***

### **Definitions:**

"BATS" refers to the web-based computer application owned and operated by ATF's USBDC to link qualified law enforcement and other public safety agencies and their approved users through a secure telecommunications medium to better facilitate the sharing of information and intelligence concerning incidents involving arson and the suspected criminal misuse of explosives. The software application is designed to operate through the computer(s) provided by the participating law enforcement/public safety agency, U.S. military or other U.S. federal/state/local governmental entities. These will be electronically linked via their local Internet Service Provider (ISP) to a Gov't provided or approved local or wide area network communications system operated as part of BATS.

"Incident" refers to: Explosions, Explosives-Related Recoveries, Suspicious/Unattended Packages, Fires, Hoax Devices, Theft of Explosives, Loss of Explosives, and Bomb/Arson Threats. This is the actual situation ***found on the scene*** upon arrival by the BATS reporting agency.



## Bomb Arson Tracking System (BATS) Rules of Behavior & User Agreement Form



**Note:** The type of incident reported in BATS may not be the same as the incident type initially dispatched. *If a more serious condition developed after arrival on the scene*, then that incident type (most serious) is to be reported in BATS. For example, if the originating call was “suspicious package” and upon arrival an IED was found, the BATS incident classification would be “Recovery > IED.”

“Activity” refers to *non-incidents* such as training, disposal / destructs, operational stand-by, administrative duties, magazine inventories/inspections, equipment maintenance, code enforcement, courtroom testimony, briefings, peer review, canine, etc.

**Note:** The Activity section in BATS is *not* intended to be used for documenting Incidents. Reporting Incidents in BATS ensures that the information is entered into the national database. This is important to the successful conclusion of a single investigation. The importance of having information in the national database is the ability to “connect the dots” to other cases or identify a particular type of device that may be associated with a known bomb maker (i.e., signature) or serial arsonist. When Incident information is incorrectly entered into the Activities section, this information is *not* available to your fellow bomb technicians and investigators when they conduct their queries of the system.

**\*\*Use of the BATS program requires that if an Activity entry is part of an Incident, that related Incident MUST also be entered into BATS.** For example: An explosives **Disposal** (Activity) of **Recovered Explosives** (Incident) or a **Fire Scene Examination** (Activity) of a **Fire** (Incident). This can be accomplished via the “Related Incidents” tab within the Activity creation screen OR via the “Related Activities” section within the Incident creation screen.

**The USBDC reserves the right to remove access to BATS due to not reporting Incidents** (see also: *Administrative*). If an agency is using BATS **solely** for the Activities section, and is not entering Incidents, or is entering Incidents as Activities, this takes away from the overall mission of BATS and uses limited valuable resources (i.e., Help Desk, USBDC resources). The agency will first be contacted and asked to remedy the situation, but may be removed from the system if they are unwilling to do so.

“Law Enforcement BATS Users” (LEBUs) refers to those persons nominated by a law enforcement or public safety agency responsible for investigating or assisting in the investigation of crimes involving fire and/or explosives for access to the BATS application and that have been expressly authorized by USBDC/ATF for such access. LEBUs must have and maintain a current National Crime Information Center (NCIC) Originating Agency Identifier (ORI) during the duration of their association with the BATS application. LEBUs will have access to BATS to document incidents and activities, advisories, and have query abilities for all of their own data, as well as other law enforcement and non-law enforcement user incident data. LEBUs agree to notify the USBDC/ATF immediately upon any change of NCIC status or use privilege.

“Non-Law Enforcement BATS Users” (NLEBUs) refers to those persons nominated by a public safety agency responsible for investigating or assisting in the investigation of incidents involving fire and/or explosives for access to the BATS application and that have been expressly authorized by ATF for such access. (NLEBUs) users will have access to BATS to document incidents and activities, and have query abilities for all of their own data, as well as other non-law enforcement user incident data. (NLEBUs) will also have access to the non-LE sensitive posted advisories and investigative resources. (NLEBUs) are not required to have an ORI, however full BATS query privileges require an ORI. Contract analysts working for a public safety agency will be considered on a case by case basis.

“ORI” (Originating Agency Identifier) is a 9-character alphanumeric CJIS-assigned criminal justice agency identifier. USBDC/ATF uses the ORI to identify a “law enforcement” agency in BATS and maintain operational security of the system. Public safety agencies that have their own ORI shall have full BATS query privileges.

“Non-LE Intel Users” from public safety or other governmental agencies will have access to limited advisories, national statistics, as well as use of the activity section. Contract analysts working for a public safety agency will be considered on a case by case basis by the USBDC.

“Military EOD Users” will have access to Explosives-related advisories, national statistics, optional incident reporting, as well as use of the activity section. Military accounts require a unit identification code (UIC), a 6-character DOD-assigned identifier unique to each unit of the Armed Forces. An ORI is required for full query access.

“Account Manager” refers to that person or persons responsible for the administration of the BATS application within the user’s agency. This includes but is not limited to authorizing new agency BATS users and coordinating BATS policy





## Bomb Arson Tracking System (BATS) Rules of Behavior & User Agreement Form



compliance for all of the agency's end-users. This should ideally be a member of supervisory rank or functional equivalent. The account manager must be designated by the agency head or designee on official letterhead, and shall include account manager's name, title, phone number, official e-mail, and official mailing address. ***The account manager is required to notify ATF and the USBDC immediately upon the lack of need for access to BATS due to retirement, transfer, reassignment, termination, and/or separation of an authorized end-user, in order to terminate their BATS account.*** A change in account manager designation to any current agency BATS user may be requested by the agency's account manager of record via official e-mail to [USBDC@atf.gov](mailto:USBDC@atf.gov). The addition of a new account manager can be authorized by the current account manager of record, or, if not available, the agency's head or designee.

"Dispatch/Support" is a limited user role for agencies that want to designate support personnel (within their agency) to make the initial BATS "incident" entry and then reassign it to the primary case owner (within their agency) to update that record. This role does not allow the "Dispatch/Support" user to search outside their agency, nor access to advisories or the "activity" section." ***Agencies electing to use this role must ensure that the incident is updated after the initial record is transferred to the case user to reflect the actual situation found on the scene.*** For example, if the originating call was "suspicious package" and upon arrival an IED was found, the BATS incident classification would be "Recovery > IED."

The "Incident Review Tool" (formerly "compliance") tab is an ***optional*** feature that provides the agency supervisor or BATS account manager with the ability to review and approve BATS "incident" entries by other members of their agency. "Review required" refers to a BATS user whose incident entries can be accepted or rejected by their agency's "compliance reviewer." The "compliance reviewer" role defaults to the "account manager" however it can be re-assigned to another unit member by contacting the USBDC. ***Agencies can opt out of this feature by sending an e-mail to [USBDC@atf.gov](mailto:USBDC@atf.gov).***

### **Scope:**

The user acknowledges that it is in the public interest to enhance cooperation among City, State, County, Tribal and Federal law enforcement & public safety agencies with regard to identifying the perpetrators of crimes involving arson and the suspected criminal misuse of explosives.

The user acknowledges that USBDC/ATF and the BATS application will assist City, State, County, Tribal and Federal law enforcement & public safety agencies in combating the crimes of arson and the suspected criminal misuse of explosives through the collection, cataloging, automated processing, comparison, and dissemination of intelligence and information; and by making available other ATF criminal and regulatory resources.

### **Access and Control of Data:**

#### Passwords and User Names

#### **\*\*Mandatory Provisions:**

- Do not write down a password or store it on a computer. Do not store any passwords on your workstation.
- NEVER give a password to another person to use or log on and never allow another person to use your log on user ID who is not authorized. You are accountable for all activities that occur using your log on user ID. The only exception to this provision is to log onto the system for the purposes of authorized maintenance or problem-solving regarding access to the BATS application by authorized personnel (system administrators or Help Desk support) – ***the Help Desk will NEVER ask for your password.***
- If your password has been compromised the user changing his/her password must nullify the exposure immediately.
- NEVER use someone else's user ID and password.

#### ***Weak passwords:***

- Habit247365# - Contains a dictionary word.
- Jaysmith91! - Contains a family member's name.
- 4URedSoxR1! - Contains the name of a sports team.

#### ***Strong passwords:***

- w\*I\*w1&20 - "When I was one and twenty"
- L%a%g%o%T% - "Let's all go outside today"
- 2P\*a\*s\*s\*2\*U - "To Pass To You"

#### **Encouraged Methods and Procedures:**

- Construct effective passwords.



## Bomb Arson Tracking System (BATS) Rules of Behavior & User Agreement Form



- Avoid obvious ones like variations of your name, your birth date, your children's names or birth dates, hobbies, sports teams, address, phone number, Social Security Number, or other personal attributes.
- Use a combination of alpha, numeric and special characters for passwords.
- Use passwords with a minimum of twelve (12) characters.
- Change passwords frequently - at least every 90 days or immediately when they may have been disclosed. Do not use one that you have used in the past.
- Enter a password only when no one else is present.
- Do not attempt to guess your user ID or password. If you have forgotten it get help from a security official. Guessing on the part of a legitimate user would falsely indicate suspicious activity to the system's audit function.
- Follow log-in procedures from start to finish without interruption.
- Never attempt to bypass or automate log in procedures that require user ID and password entry.
- Be alert to unauthorized attempts to use your user ID & password. ***Immediately report unauthorized attempts to the USBDC or the Help Desk.***
- Logout of the BATS application whenever you leave the vicinity of your workstation.

### Sensitive But Unclassified Law Enforcement Data

As a national repository of incident-based information, BATS contains Sensitive But Unclassified (SBU) in the Information Sharing Environment (ISE). ***Failure to protect and safeguard such data from loss, misuse, or unauthorized access could adversely affect law enforcement operations, including those areas related to officer safety as well as the fair and equitable administration of justice, and the privacy of individuals.***

### **\*\*Mandatory Provisions:**

- Data derived from BATS is SBU law enforcement data and should be protected against loss, compromise, or misuse.
- Only use data for which you have been granted authorization, do not attempt to gain access to information to which you do not have the authority.
- Don't retrieve information from a system for someone who does not have authority to access the information; only give information to people who have access authority and who need the information in the performance of their ***official duties***.
- Do not allow unauthorized or unescorted personnel into an area where SBU law enforcement information is processed. Report any unauthorized personnel to the appropriate authority.
- Abide by procedures as outlined in the user agreement governing the channels for requesting/disseminating information.
- Avoid unauthorized "browsing," namely, only access information directly related to your ***official duties*** even though you may be allowed to access it.

### Encouraged Methods and Procedures:

As the BATS software application allows local systems account managers of participating agencies the ability to export records that they have contributed, the following are encouraged methods for the handling of such information:

- Take the same care with system output as with the system itself, that is, control access to printouts, disks, tapes or other media storage devices that contain your BATS software application records.
- Lock up/secure storage media/hard copy containing your BATS software application records at the end of the day or when otherwise unattended.
- Do not leave computer printouts containing your BATS software application records unattended at printers.
- Mark media to readily distinguish your BATS software application records from other files.
- Dispose of workstation disks, including hard drive disks, containing your BATS software application records by erasing sensitive data, degaussing, shredding, or following other appropriate procedures.

### **Operating Parameters:**

Each agency is responsible for administering and making entries into their BATS account. ***BATS users are encouraged to enter into the BATS application all relevant information based on their agency's response and/or investigative involvement in incidents related to arson, and the suspected criminal misuse of explosives.*** Since it has been the experience of ATF that incendiary or arson related fires can be mistakenly characterized as accidental fires, BATS users should contribute all fire and explosion incidents including those initially classified as accidental and undetermined. ***Users are strictly prohibited from knowingly entering inaccurate or false information, even if it's to become familiar with BATS. Doing so may not only result in a revocation of BATS use privileges, but may also expose you adverse action or liability. Note: Users can request access to the BATS training site by contacting the USBDC at [USBDC@atf.gov](mailto:USBDC@atf.gov)***

The user acknowledges that information contributed to the BATS application must be classified by the user on an individual incident basis in the following manner:



## Bomb Arson Tracking System (BATS) Rules of Behavior & User Agreement Form



### Restricted (end-user selected)

In the event information contributed by the user matches a query developed and executed by an outside agency that is also a participant in the BATS application, only contact information such as: Case Number, Agency, Investigator /Agent, Agency Name, Agency City, Agency State, Agency Telephone Numbers will be released concerning the identified record. Juvenile data is automatically marked as restricted.

### Unrestricted (end-user selected)

In the event information contributed by the user matches a query developed and executed by an outside agency that is also a participant in the BATS application, all information within the system concerning an identified record will be accessible in a non-modifiable (read-only) form. Juvenile data is automatically marked as restricted.

### Specific Unrestricted Access (end user-selected)

The user can grant "read-only" or "write" access to another investigator or task force allowing them to collaborate on a particular "incident."

### **BATS Application Information Reliability:**

The user is responsible for and shall take those steps necessary to ensure the accuracy of information contributed to BATS is based on their agency's response and/or official investigative involvement in incidents related to arson, and the suspected criminal misuse of explosives

The user hereby agrees that use of information from the system shall be considered only as an investigative tool. ***Files and other information entered into BATS are not considered original documents and are to be maintained by each contributing agency.*** Users are encouraged to follow their local rules of evidence governing the storage of electronic media. ATF cautions that data obtained from the system is not to be used as admissible evidence in any proceeding without coordinating with and further verifying such information with the agency that contributed the information in question. See also *disclosure/dissemination*.

### **Data Integrity:**

Reliable data is critical to the successful operation of any law enforcement information system. The following mandatory provisions will ensure the reliability of incident based information contributed to the BATS program:

### **\*\*Mandatory Provisions:**

- All users of the system shall take those steps necessary to ***ensure the accuracy*** of any information contributed.
- Information derived from the BATS application should be considered ***only as an investigative tool***. It is recommended that any data obtained from the BATS application be ***verified with the agency that contributed the information***.
- ***Prevent*** unauthorized alteration, damage, unauthorized destruction, or tampering with BATS application or the information contained within it.
- ***Never enter unauthorized, inaccurate, or false information***, and remove such information if discovered after entry.
- Do not manipulate information inappropriately.
- Create only authorized records or files.
- ***Avoid browsing*** data you have no official need to see.
- Protect workstations and electronic storage devices from theft.

### **User Responsibility:**

#### Disclosure/Dissemination

The user acknowledges that information pertaining to individuals is based on their suspected criminal involvement or as witnesses or victims in criminal case investigations and law enforcement concerns. Criminal activity includes juvenile acts that if committed by an adult would be a crime. ***This is case data collected by Law Enforcement and public safety in the performance of their duties and is within the scope of the Privacy Act exemption for law enforcement records pursuant to 5 U.S.C. § 552a(j)(2). See also FOIA's law enforcement exemptions, 5 U.S.C. 552(b)(7).***

The user acknowledges that ***no*** information contained within the BATS application will be disclosed to a third party except as described in this agreement. The user agrees that the agency contributing information into BATS is the custodian/owner of that record and will abide by their own state laws, statutes, and regulations and maintain that data accordingly. The user agrees there will be no disclosure of information contributed by the user's agency into BATS outside of the user's agency except that disclosure which is deemed necessary by ATF and the USBDC or the user's agency in conjunction with an



## **Bomb Arson Tracking System (BATS)** Rules of Behavior & User Agreement Form



official law enforcement investigation or pursuant to a lawful court order or legal request (including discovery requests). ***Such disclosure shall only apply to incident information that the user's agency has contributed into BATS.*** The use of BATS in and of itself by an authorized agency, does not actively involve ATF or the USBDC in the investigation or the prosecution of a particular incident. The user agrees to immediately report to ATF and the USBDC any order that it might receive arising from a legal proceeding that is issued by a court of competent jurisdiction ordering the disclosure of information contained within the BATS application that was contributed by an agency other than the user's agency.

The user also agrees that disclosures made under a user's State Public and Open Records Laws (including arson immunity laws) or other internal agency dissemination policy ***apply only to incident reports that the user's agency has contributed into BATS.*** See also 5 U.S.C. 552(b) (7), which generally exempts from disclosure "records or information compiled for law enforcement purposes." The user agrees to immediately report to ATF and the USBDC any such request that it receives which seeks the disclosure of information contained within the BATS application that was contributed by a participating agency other than the user's agency. ***ATF does not process public records requests for records contributed to BATS by non-ATF agencies.***

The user agrees that ***premature disclosure of certain information resident within the BATS application other than as described in the preceding paragraphs can reasonably be expected to interfere with pending or prospective law enforcement operations and/or prosecution proceedings.*** This law enforcement sensitive information includes but is not limited to data that may link a person or persons to an incident or incidents; criminal methodology of an incident or incidents; personally identifiable information; ORI information, or information related to patterns of criminal activity involving arson and the suspected criminal misuse of explosives. The user agrees that the above described law enforcement sensitive information shared or generated pursuant to this agreement shall not be disclosed to any party except as described in this agreement without the express consent of both parties to this agreement.

***Any advisories or reports (including the information contained within them) obtained from the BATS system or ATF and the USBDC may only be further disseminated in accordance with the document's designation.*** Law Enforcement Sensitive (U//LES) may only be disseminated to federal, state, tribal, or local government law enforcement. For Official Use Only (U//FOUO) may only be disseminated to U.S. federal, state, tribal, local government, or military officials.

### **Costs:**

***The use of the BATS system is free-of-charge to participating agencies.*** The user agrees that ATF and the USBDC are not responsible for costs or liabilities associated with an agency's computer hardware, computer software (other than the BATS application), Internet connection(s), or other communications requirements associated with their use of the BATS application. ATF and the USBDC will maintain access to the BATS application furnished to the user and shall facilitate repairs to the BATS application in an expeditious manner, subject to availability and funding. However, maintenance or repairs required as the result of improper use of the BATS application by the user or enhancements to the BATS application by the user, as well as repairs to local computer hardware, computer software, or communications problems, will not be assumed by ATF.

### **System Access:**

The user hereby agrees to notify ATF and USBDC ***immediately upon the lack of need for access to BATS due to retirement, transfer, reassignment, termination, and/or separation*** of an authorized end-user, in order to terminate their BATS account.

The user agrees that BATS will only be accessed through computers owned or leased for official government purposes. The user agrees that ATF and the USBDC retain all proprietary rights to include but not limited to the BATS schema and computer code.

The user agrees that access to the BATS via any type of wireless communication medium or appliance must be protected by authentication to ensure protection from unauthorized system access. Wireless devices shall support a minimum of 128-bit encryption with NIST or CSE certification of the cryptographic module to ensure it meets FIPS Publication 140-2 for Security Requirements for Cryptographic Modules.

### **Administrative:**

ATF retains the right to remove access to the BATS application upon (1) its determination that the BATS application is being neglected or misused, or is not receiving use to a reasonable degree; (2) receipt of written notification of the termination by participating agency; or (3) termination of the BATS application by the USBDC.





**Bomb Arson Tracking System (BATS)**  
Rules of Behavior & User Agreement Form



The user acknowledges that the operations described in this agreement are subject to audit by ATF; the U.S. Department of Justice; Office of Inspector General; the General Accounting Office; and other auditors designated by the U.S. Gov't. Such audits may include reviews of any and all records, documents, reports, accounts, invoices, receipts, and other evidence. The user acknowledges that, for accounting purposes, the principles and standards for determining costs shall be governed by the policies set forth in the Office of Management and Budget (OMB) Circular A-87, revised (available via the OMB, The Superintendent of Documents at the U.S. Government Printing Office, or via the Internet at <http://www.whitehouse.gov/WH/EOP/OMB>).

**Miscellaneous Provisions:**

The user agrees to immediately report to ATF and the USBDC any incident involving unauthorized alteration, damage, or destruction of ATF-owned BATS application; any unauthorized use or access of the BATS application; or the unauthorized release of information related to the BATS application. **\*\*BATS users are encouraged to add [USBDC@atf.gov](mailto:USBDC@atf.gov) to their "safe senders" list in order to prevent USBDC/BATS messages from being marked as spam.**

**Duration:**

The terms and conditions of this agreement will be considered accepted in their entirety upon the signature by the user and may be amended by deletion or modification, or by addition of new provisions, by ATF and the USBDC. If this project is terminated by either party, ATF and the USBDC will retain their interest in the electronically stored information contained in the database, except that USBDC/ATF agrees to provide a copy of the data contributed by the agency.

The USBDC/ATF or participating agency may cancel its participation at any time following written notification to the other party.

**Effect of Agreement:**

Nothing in this agreement will modify any Federal law, regulation, or other Federal rule. Nothing in this agreement grants any funding, whatsoever. All specific actions agreed to herein shall be subject to funding and administrative or legislative approvals. The user acknowledges that financial and civil liability, if any, and in accordance with applicable law, for the acts or omissions of each party's employees, remains vested with his or her employing agency. No third party is intended to benefit or otherwise claim any rights whatsoever under this agreement.

The user hereby agrees to abide by the terms and conditions of this agreement to participate in the BATS application in the manner prescribed herein; to use it in a manner prescribed herein; to allow the necessary and proper administration of the program; and to comply with all conditions that ATF/USBDC may find necessary to institute on behalf of the BATS application.

Failure to comply with the above mandatory rules of behavior will be considered a security incident. If the incident is deemed willful, it will be escalated to a security violation. Depending on the number of security violations and the sensitivity of the information involved, your access to the BATS application may be revoked and/or the ability of your agency to participate in the BATS program may be terminated. In addition, the aforementioned does not preclude potential civil or criminal penalties.

***By signing below, I certify that I have read, understand, and will comply with this user agreement for access and use of the BATS program.***

Date: \_\_\_\_\_

User's Printed/Typed Name: \_\_\_\_\_

Last 4 of SSN (####): \_\_\_\_\_

Agency / Office: \_\_\_\_\_

User's Signature: \_\_\_\_\_



 Account Manager's Signature: \_\_\_\_\_

***(must also sign Access Form\*)***



\*\*\*Please fax this page **PLUS** the **\*Access Request Form\*** to the USBDC @ 866-927-4570, attn: BATS Unit.



**\*\* AVOID DELAYS – USE THE APPLICATION CHECKLIST \*\***  
*(see second page)*

