Department of the Treasury
BUREAU OF ENGRAVING AND PRINTING

Digital Video Recording System (DVRS)

November 4, 2011

A. Contact Information

System/Project Name	Digital Video Recording System (DVRS)
OMB Unique Identifier	Not applicable

1. Who is the person completing this document?	
Name / Title	Lynn Henderson; Cyber Architect VI
Office/Division	Office of Critical Infrastructure and IT Security (OCIITS)
Phone Number	202-847-0826
Email Address	Lynn.Henderson@bep.gov

2. Who is the system owner?	
Name / Title	Will Levy III, Chief of Security
Office/Division	Security
Phone Number	202-874-3633
Email Address	Will.LevyIII@bep.gov

3. Who is the system manager for this system or application?	
Name / Title	Will Levy III, Chief of Security
Office/Division	Security
Phone Number	202-874-3633
Email Address	Will.LevyIII@bep.gov

4. Who is the Information System Security Manager who reviewed this document?	
Name / Title	Harinder Singh
Office/Division	Office of Critical Infrastructure and IT Security (OCIITS)
Phone Number	202-874-0003
Email Address	Harry.Singh@bep.gov

5. Who is the Office/Bureau Privacy Officer who reviewed this document?	
Name / Title	Keir Bancroft; Attorney-Advisor
Office/Division	Office of the Chief Counsel
Phone Number	202- 874-5915
Email Address	Keir.Bancroft@bep.treas.gov

6. Who is the IT Reviewing Official?	
Name / Title	David Redding; Manager, IT Audit and Compliance Division
Office/Division	Office of Critical Infrastructure and IT Security (OCIITS)
Phone Number	202-874-2953
Email Address	David.Redding@bep.gov

B. System Application/General Information

1. **Does this system contain any PII? [ ] No [X] Yes**

2. **What is the purpose of the system/application?**

   The Digital Video Recording System (DVRS) is designed to capture, manage and store video from the Bureau of Engraving and Printing's ("BEP's) video camera network. DVRS, a physical security system, is a combination of hardware and software technologies that digitize, compress, record, store, and manage digital video, and provide capability to view live and recorded data from user workstations. Information is used for security alerting and BEP Security personnel activity. The DVRS records individuals' entrance and exit to the building and to sensitive or restricted access areas. Users may also enter text notes into the system.

3. **What legal authority authorizes the purchase or development of this system/application?**

   Executive Order 10450, Sections 2 and 3, Executive Order 12958, Executive Order 12968, and Homeland Security Presidential Directive 12; 31 U.S.C. 321; 5 U.S.C. 301, and 5 U.S.C. 6106.

4. **Under which SORN does the system operate? (Provide name and number)**

   The authorities, categories of individuals, categories of records, purposes, routine uses, and policies and practices for storing, retrieving, accessing, retaining, and disposing of records in this system align with and fall under the following series of SORNs:

   Treasury .007 – Personnel Security System
   Treasury/BEP .021 – Investigative Files
   Treasury/BEP.027 - Access Control and Alarm Monitoring Systems (ACAMS)

C. Data in the System

1. **What categories of individuals are covered in the system? (e.g., employees, contractors, taxpayers, other)**

   Employees, contractors and members of the general public within the range of the system's interior and exterior video cameras may be recorded with this system.

2. **What are the sources of information in the system?**

   a. **Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other sources?**

This system makes video recordings of specified spaces within and surrounding BEP buildings. The system records the likeness of individuals located within the spaces being recorded. Additionally, the BEP Security personnel may access personnel records for the purpose of annotating notes.

Although 10 or more people may be covered by this system, it is not subject to the Paperwork Reduction Act because it does not directly collect information from the persons recorded, and any notes are not recorded in formatted records (e.g., database schema, spreadsheet).

b. What Federal agencies are providing data for use in the system?

The only Federal agency providing data for use in the system is BEP.

c. What state and/or local agencies, tribal governments, foreign governments, or international organizations are providing data for us in the system?

No states, local agencies or other entities will provide data for use in this system.

d. From what other third party sources will data be collected?

Other sources from which data may be collected are referenced in Section 2.a. above.

e. What information will be collected from employees, government contractors and consultants, and the public?

The information that is collected from employees, government contractors and consultants, and the public will be video imagery of a person's likeness. However, the video may be supplemented by added notes captured in the system that may pertain to an individual's identity.

3. Accuracy, Timeliness, and Reliability

a. How is data collected from sources other than from Treasury records going to be verified for accuracy?

Data is gathered at the point of collection, i.e. interviews.

b. Is completeness required? [X] No []Yes

Notes will be recorded with as much completeness as deemed required by BEP security personnel.

c. What steps or procedures are taken to ensure the data is current and not out-of-date?

All video recorded via the DVRS is date and time stamped. If a note is added to the system, it may be associated with the appropriate date/time stamp to associate it with a video likeness.

d. Are the data elements described in detail and documented? [X] No [ ] Yes

This is not applicable as the notes are written in free form. There is no set format for the authoring notes.

D. Attributes of the Data

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

   Yes. Information is used for security alerting and law enforcement activity.

2. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? [ ] No [X] Yes**

   Information captured in the notes feature may be manually obtained from systems and or individuals.

3. **Will the new data be placed in the individual's record? [X] No [ ] Yes**

4. **Can the system make determinations about employees/members of the public that would not be possible without the new data?**

   No, the system only captures video and text data; it does not analyze it.

5. **How will the new data be verified for relevance and accuracy?**

   Data will be verified for relevancy and accuracy in accordance with the information referenced in C.3.a, b, and c above.

6. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   Automated access controls restrict access from unauthorized users, and audit logs track activities of authorized users for non-repudiation as a preventative control.

7. **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

   Access is limited to authorized users.

8. **How will the data be retrieved? Is the data retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

   Video data is recorded on a DVR and can be played back. Video is date/time stamped to facilitate search. Notes are freeform text and may be searched using keyword search.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   The system does not produce reports on individuals.

E. <u>Maintenance and Administrative Controls</u>

1. **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

   System operating procedures are provided to system users. Data will only be used for the purpose it was collected.

2. **What are the retention periods of data in the system?**

   The system has capacity to store one year's worth of data. The system can be set to overwrite the data or stop recording when it reaches capacity.

   Audit reports are stored as part of the e-mail archives in the ITAUDIT@bep.gov mailbox. Audit trails will be recorded and retained in accordance with the Bureau's Record Management Program, and are maintained and available for a minimum of 5 years.

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

   Data is overwritten when the system reaches its one-year capacity. No reports are produced. Data extracts (on CD or DVD) created by request in support of law enforcement or administrative investigation are the responsibility of the requestor. There are no data retention procedures.

4. **Is the system using technology in ways the office or bureau has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, explain.**

   No

5. **How does the use of this technology affect public/employee privacy?**

   Information captured by DVRS will be used for no purpose other than legal or administrative matters as described in the SORNs above.

6. **Will the system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

   DVRS supports the ability to identify, locate and monitor individuals located in areas monitored by video cameras. The DVRS does not directly identify individuals. However, if the DVRS captures a readable likeness of an employee or contractor badge, the video could also be used to assist in identifying the individual. The notes capability enables BEP Security personnel to record the identity of individuals if known by the video observer or researched through sources external to DVRS.

7. **What kind of information is collected as a function of the monitoring of individuals?**

   The likeness of an individual is recorded in video recordings, and BEP Security personnel may record text notes associated with the video recordings concerning an individual's identity or actions.

8. **What controls will be used to prevent unauthorized monitoring?**

   Unauthorized monitoring will be prevented by both the access and physical controls that have been put in place. The physical location of the cameras ensures that only appropriate areas are being monitored. Additionally, DVRS is a controlled system and is limited to authorized users of the BEP Police Force in support of their duties. Access controls prevent unauthorized users from using the system.

9. **Under which SORN does the system operate? (Provide name and number)**

   As noted under section B.4 above, The authorities, categories of individuals, categories of records, purposes, routine uses, and policies and practices for storing, retrieving, accessing, retaining, and disposing of records in this system align with and fall under the following series of SORNs:

   Treasury .007 – Personnel Security System
   Treasury/BEP .021 – Investigative Files
   Treasury/BEP.027 - Access Control and Alarm Monitoring Systems (ACAMS)

10. **If the system is being modified, will the SORN require amendment or revision? Explain.**

    The system is not being modified; it is a new system that is being prepared for deployment. If it is determined that the cited SORNs require any amendment or revision due to use or modification of the system, they will be amended or revised accordingly.

F. Access to Data

1. **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others).**

   BEP Federal employee law enforcement personnel system users, contractors, managers and system administrators will all be able to access this system. Additionally, data exports may be provided to Federal, State and Local law enforcement upon request.

2. **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

   Access to the data in the system is controlled by user access controls (identification and authentication). Access controls are documented in the DVRS System Security Plan.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   Authorized users have access to all data on this system.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? List procedures and training materials.**

   The purpose of the system is to provide users (BEP Security personnel) to view any data captured by video cameras in the conduct of their physical security responsibilities. However, the capability to export video from a camera to the workstation and save on the workstation hard drive is restricted by the Video Management System (VMS) software to a limited number of users; and the capability to burn a DVD is also restricted to a limited number of users by the VMS user settings. Both capabilities are required to export data to a DVD. Audit logs (a deterrent control) capture both events.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

   Yes. The prime contractor for the system is Johnson Controls Security Services who is responsible for installation and maintenance of the commercial-off-the-shelf (COTS) DVRS system developed and maintained by Aventura. Aventura implements and tests their system changes and Microsoft patches in their lab before submitting the changes to Johnson Controls for installation in the system.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

   DVRS does not share data or have access to any other systems at this time; i.e., there are no system interfaces.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The system owner, Will Levy III, will be responsible for protecting the privacy rights of the public and BEP employees and contractors.

8. **Will other agencies share data or have access to the data in this system?**

[X] Federal [X] State [X] Local [X] Other

9. **How will the data be used by the other agency?**

Information captured by DVRS will be used by BEP for no purpose other than legal or administrative matters as described in the SORNs above. Agencies with which this data may be shared will use this data as appropriate for legal and administrative purposes.

10. **Who is responsible for assuring proper use of the data?**

The system owner, Will Levy III, in coordination with the Office of the Chief Counsel and corresponding roles of data recipients, are responsible for assuring proper use of data collected by DVRS.

The Following Officials Have Approved This Document

1. **Program Manager**

   Name: Will P. Levy III

   Date 11/4/11

2. **System Manager**

   Name: Will P. Levy III

   Date 11/4/11

3. **Information System Security Manager**

   Name: Harinder Singh

   Date 11-4-11

4. **Privacy Officer**

   Name: Keir Bancroft

   Date 11/4/11

5. **IT Review Official**

   Name: David Redding

   for David Redding Date 11/4/11

6. **Deputy Assistant Secretary for Privacy and Treasury Records (when necessary)**

   Name: Melissa Hartman (if applicable)

   N/A Date