



Affects Members Of the Public?

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, *Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments*, for requirements and additional guidance for conducting a PIA: <http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf>

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	May 14, 2015	
Departmental Element & Site	Bonneville Power Administration Portland, Oregon	
Name of Information System or IT Project	Ocularis	
Exhibit Project UID	BPA is a self-funded Federal agency and is exempt from Exhibit 300 submissions.	
New PIA	<input checked="" type="checkbox"/>	
Update	<input type="checkbox"/>	
	Name, Title	Contact Information Phone, Email
Information System Owner	Yvette Gill Supervisory IT Specialist	(503)230-3947 yrgill@bpa.gov
Information Owner	Lee Hall Chief Security and Continuity Officer	(503)230-5189 ljhall@bpa.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Christopher Frost Privacy Officer	(503)230-5602 cmfrost@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Darren Jungling IT Specialist	(503)230-3553 dljungling@bpa.gov
Person Completing this Document	Nicholas Heller IT Specialist	(360)839-8905 nmheller@bpa.gov
Purpose of Information System or IT Project	Ocularis is a video management system that combines network video records (NVRs) with physical security by providing an interface to turn recorded events into meaningful alerts that can be managed by the security staff.	
Type of Information Collected or Maintained by the System:	<input type="checkbox"/> SSN Social Security number <input type="checkbox"/> Medical & Health Information e.g. blood test results <input type="checkbox"/> Financial Information e.g. credit card number <input type="checkbox"/> Clearance Information e.g. "Q" <input type="checkbox"/> Biometric Information e.g. finger print, retinal scan <input type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> DoB, Place of Birth <input type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input type="checkbox"/> Name, Phone, Address <input checked="" type="checkbox"/> Other – Please Specify: Digital video of individuals	
Has there been any attempt to verify PII does not exist on the	N/A	



MODULE I – PRIVACY NEEDS ASSESSMENT

<p>system?</p> <p>DOE Order 206.1, <i>Department of Energy Privacy Program</i>, defines PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.</p>	
<p>If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)</p>	N/A

Threshold Questions

<p>1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?</p>	YES
<p>2. Is the information in identifiable form?</p>	YES
<p>3. Is the information about individual Members of the Public?</p>	YES
<p>4. Is the information about DOE or contractor employees?</p>	<p>YES</p> <p><input checked="" type="checkbox"/> Federal Employees</p> <p><input checked="" type="checkbox"/> Contractor Employees</p>

If the answer to **all** four (4) Threshold Questions is "No," you may proceed to the signature page of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.



MODULE I – PRIVACY NEEDS ASSESSMENT

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

<p>1. AUTHORITY What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?</p>	<p>16 U.S.C. § 839f(b)</p>
<p>2. CONSENT What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?</p>	<p>NONE</p>
<p>3. CONTRACTS Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?</p>	<p>NO</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>4. IMPACT ANALYSIS: How does this project or information system impact privacy?</p>	<p>The potential impact is MODERATE.</p> <p>The potential for privacy concerns if the system is compromised could be expected to have a serious adverse effect on individuals.</p> <table border="1" data-bbox="609 552 1485 1318"> <thead> <tr> <th rowspan="2"></th> <th colspan="3">Impact Level</th> </tr> <tr> <th>Low</th> <th>Moderate</th> <th>High</th> </tr> </thead> <tbody> <tr> <td>Confidentiality Factors</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Identifiability</td> <td></td> <td></td> <td>X</td> </tr> <tr> <td>Quantity of PII</td> <td></td> <td></td> <td>X</td> </tr> <tr> <td>Date Field Sensitivity</td> <td>X</td> <td></td> <td></td> </tr> <tr> <td>Context of Use</td> <td></td> <td>X</td> <td></td> </tr> <tr> <td>Obligation to Protect Confidentiality</td> <td>X</td> <td></td> <td></td> </tr> <tr> <td>Access to and Location of PII</td> <td></td> <td>X</td> <td></td> </tr> <tr> <td>Overall PII Confidentiality Level</td> <td></td> <td>X</td> <td></td> </tr> </tbody> </table>		Impact Level			Low	Moderate	High	Confidentiality Factors				Identifiability			X	Quantity of PII			X	Date Field Sensitivity	X			Context of Use		X		Obligation to Protect Confidentiality	X			Access to and Location of PII		X		Overall PII Confidentiality Level		X	
	Impact Level																																							
	Low	Moderate	High																																					
Confidentiality Factors																																								
Identifiability			X																																					
Quantity of PII			X																																					
Date Field Sensitivity	X																																							
Context of Use		X																																						
Obligation to Protect Confidentiality	X																																							
Access to and Location of PII		X																																						
Overall PII Confidentiality Level		X																																						
<p>5. SORNs How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>The data is not routinely retrieved by a personal identifier. Because records in this system are not routinely retrieved by personal identifier, the Privacy Act does not apply to this system and there is no applicable System of Records. A System of Records Notice is not required.</p>																																							



MODULE II – PII SYSTEMS & PROJECTS

6. SORNs Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i> ? If "Yes," provide name of SORN and location in the <i>Federal Register</i> .	N/A. The Privacy Act does not apply to this system.
7. SORNs If the information system is being modified, will the SORN(s) require amendment or revision?	N/A. The Privacy Act does not apply to this system.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Direct from video of individuals.
9. Will the information system derive new or meta data about an individual from the information collected?	NO
10. Are the data elements described in detail and documented?	YES, in the System Security Plan
DATA USE	
11. How will the PII be used?	PII collected from Ocularis is assessed by BPA security staff if an alert is triggered within the security system. Ocularis data is used to validate the alert or identify nuisance alarms. Data may also be provided to Law Enforcement to identify individuals involved in an investigation.



MODULE II – PII SYSTEMS & PROJECTS

12. If the system derives meta data, how will the new or meta data be used? Will the new or meta data be part of an individual's record?	N/A
13. With what other agencies or entities will an individual's information be shared?	Potentially, a warrant could compel BPA to share collected video with Law Enforcement.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	NONE
15. What will be the use of these reports?	N/A
16. Who will have access to these reports?	N/A
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	YES
18. What kinds of information are collected as a function of the monitoring of individuals?	Digital Video Recordings of BPA facilities and individuals within them.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	YES. Controls are provided within Ocularis as to which user roles are allowed to access digital video records within the system. Active Directory LDAP permissions and Kerberos authentication are used for any accessible share.



MODULE II – PII SYSTEMS & PROJECTS

DATA MANAGEMENT & MAINTENANCE

<p>20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.</p>	<p>The data is maintained within the Raspberry NVR. Users are validated every quarter between the Information Owner and Information System Owner.</p>
<p>21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?</p>	<p>N/A</p>
<p>Records Management</p>	
<p>22. Identify the record(s).</p>	<p>The Ocularis system is considered a Structured Electronic Information System (SEIS), which requires a SEIS – Description and Retention Schedule form (BPA F 1324.02e) to be completed and approved. However, although the system has not yet been formally scheduled, the following disposition authority is recommended (see 23 below).</p>
<p>23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.</p>	<p>Unscheduled.</p> <p>Disposition Authority(s) (proposed): N1-305-07-1-15/b & 15/c.</p> <p>Retention Period(s) (per authority):</p> <ol style="list-style-type: none"> 1. For incident/event cases tracking serious security incidents not pertaining to criminal activity, such as: altering security systems, suspected sabotage, and other incidents of a potentially serious nature: N1-305-07-1-15/b: Retain while Active* + 5 years, then destroy. 2. For incident/event cases involving vandalism, theft, explosions, fires, accidents, and other security related events: N1-305-07-1-15/c: Retain while Active* + 10 years, then destroy. <p>*Active period ends upon termination of inquiry/investigation when the case is closed.</p>
<p>24. Records Contact</p>	<p>Jeff C. Johnson, Records Analyst (503)230-5254 jcjohnson@bpa.gov</p>



MODULE II – PII SYSTEMS & PROJECTS




ACCESS, SAFEGUARDS & SECURITY

25. What controls are in place to protect the data from unauthorized access, modification or use?	There is a valid Authority to Operate in place.
26. Who will have access to PII data?	All authorized users within the system
27. How is access to PII data determined?	Access is restricted based on approval from the Information Owner.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	NO
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	The Information Owner

END OF MODULE II



SIGNATURE PAGE

	Signature	Date
Information System Owner	Yvette Gill (Print Name)  (Signature)	<u>6/9/15</u>
Information Owner	Lee Hall (Print Name)  (Signature)	<u>6/4/15</u>
Local Privacy Act Officer	Christopher Frost (Print Name)  (Signature)	<u>6/9/2015</u>
Jerry Hanley Chief Privacy Officer	Jerry Hanley (Print Name) (Signature)	