



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Department of Energy Payroll Processing (DPP)

Affects Members Of the Public? Mark if Applicable w/ an X

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: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder-chg1-minchg/@_images/file.

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	April 17, 2023	
Departmental Element & Site	Office of the Chief Financial Officer, Headquarters - Office of the Chief Information Officer (OCIO) EITS Data Center and Cloud Services (DCCS) environment	
Name of Information System or IT Project	Department of Energy Payroll Processing (DPP)	
Exhibit Project UID	019-000000122	
New PIA <input type="checkbox"/>	This is an updated PIA from the one approved on January 27, 2022. Minor editorial changes have been made and several pages have been updated with the names of new officials.	
Update <input checked="" type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
System Owner	Logan Kwedar Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	(301) 903-2145 Logan.Kwedar@hq.doe.gov



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Department of Energy Payroll Processing (DPP)

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Ana Manchester Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-9360 Ana.Manchester@hq.doe.gov
Cyber Security Expert reviewing this document (e.g., ISSM, CSSM, ISSO, etc.)	Robert Baring, ISSO Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	240-243-5796 robert.baring@hq.doe.gov
Person Completing this Document	Robert Baring, ISSO Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	240-243-5796 robert.baring@hq.doe.gov
Purpose of Information System or IT Project	<p>The Department of Energy Payroll Processing (DPP) manages payroll services for the entire U.S. Department of Energy (DOE). DPP implements the DOE portion by collecting payroll data from over 48 DOE sites and delivering the collected information to the Defense Finance and Accounting Service (DFAS), which is operated by the U.S. Department of Defense (DOD).</p> <p>DPP processes SSN and Clearance Information for DOE Employees and some contractors. DPP processes employment related data for DOE. DPP processes much more limited information for some contractors including employer name.</p> <p>DPP employs a set of internal controls to ensure the accuracy and currency of information contained in the system in light of new additions or deletions from payroll or changes in pay. DPP is composed of its software, scripts, and temporary files. DPP accesses but does not include database information hosted by the Office of the Chief Information Officer (IM). These are hosted by IM virtual servers, which offer the inheritance of multiple physical and operating system level security controls. DPP does not include the hosting servers, which are authorized separately by IM.</p> <p>DPP uses Energy Information Technology Services (EITS) Active Directory accounts to control all System Administrator access for the administration of the system. All DPP access is remote. All System Administrator account access is authorized prior to granting access. All DPP functionality is privileged. DPP restricts privileged accounts exclusively to authorized DPP support personnel.</p>	



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Department of Energy Payroll Processing (DPP)

MODULE I – PRIVACY NEEDS ASSESSMENT

Type of Information Collected or Maintained by the System:	<input checked="" type="checkbox"/> Social Security Number (SSN) <input checked="" type="checkbox"/> Medical & Health Information <input checked="" type="checkbox"/> Financial Information - Employee’s disability information and Health Benefits Plan <input checked="" type="checkbox"/> Clearance Information <input type="checkbox"/> Biometric Information <input type="checkbox"/> Mother’s Maiden Name <input checked="" type="checkbox"/> Date of Birth <input type="checkbox"/> Place of Birth <input checked="" type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name, Phone, Address <input checked="" type="checkbox"/> Other – Potential Personally Identifiable Information (PII): Security Questions/Responses (chosen and populated by employee)
---	---

Has there been any attempt to verify PII does not exist on the system? <i>DOE Order 206.1, Department of Energy Privacy Program, 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.</i>	N/A
---	-----

If “Yes,” what method was used to verify the system did not contain PII? (e.g., system scan)	N/A
---	-----

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	Yes
2. Is the information in identifiable form?	Yes
3. Is the information about individual Members of the Public?	No
4. Is the information about DOE or contractor employees?	Yes, the system contains information about current and former DOE federal



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Department of Energy Payroll Processing (DPP)

MODULE I – PRIVACY NEEDS ASSESSMENT

employees. It also contains some information on contractors that are responsible for operating the system (i.e., timekeepers and application support staff).

- Federal Employees
- Contractor Employees

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.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Department of Energy Payroll Processing (DPP)

MODULE II – PII SYSTEMS & PROJECTS

1. AUTHORITY What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?	<ul style="list-style-type: none"> Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq. 50 U.S.C. 2401 et. seq.
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>Data provided via a corporate repository (DOEInfo) contains information on the DOE Federal workforce obtained from individuals. DPP accesses information therefrom as a condition of employment for the sole purpose of facilitating compensation.</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>Contractors are involved in the design, development, and maintenance of the system. Contractor roles include both system administration and information administration and processing. Personal information may be disclosed to these contractors and their officers and employees in performance of their contracts. The individuals provided this type of information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a.</p> <p>Contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.</p>



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Department of Energy Payroll Processing (DPP)

MODULE II – PII SYSTEMS & PROJECTS

<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>DOE has assessed the system as moderate risk according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised.</p> <p>The unauthorized disclosure of information is expected to have a serious adverse effect on individuals. DPP contains sensitive PII on DOE employees including SSN and limited financial information for payroll purposes. Should this information be compromised, it would pose a potentially significant risk to individuals and could result in professional or financial harm stemming from the loss or exposure of financial information, employment information including clearance data, and SSN.</p> <p>DPP is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:</p> <ul style="list-style-type: none">• Strict access control enforcement based on need-to-know• Encryption <p>Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of the data being compromised. These include technical controls as well as role-based access controls, further restricting System Administrators to authorized data.</p>
<p>5. SORNs</p> <p>How will the data be retrieved? Can PII be retrieved by an identifier (e.g., name, unique number or symbol)?</p> <p>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>PII data can be retrieved through elevated privilege accounts within the DPP system through the following identifiers: SSN, GUID, GUID16, EMPNUM and DOE_EMPLID.</p>



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Department of Energy Payroll Processing (DPP)

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>.	<ul style="list-style-type: none"> DOE-13, Payroll and Leave Records, 74 FR 1012 DOE-18, Financial Accounting System, 74 FR 1020
7. SORNs If the information system is being modified, will the SORN(s) require amendment or revision?	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	Data is provided through an interface with a corporate repository (DOEInfo).
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. These data elements are addressed in the system documentation for DPP.
DATA USE	
11. How will the PII be used?	All data collected is used by DFAS for internal Departmental reporting (CF-10) and to ensure that individuals are accurately paid.
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?	The system does not generate new or meta data.



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Department of Energy Payroll Processing (DPP)

MODULE II – PII SYSTEMS & PROJECTS

13. With what other agencies or entities will an individual's information be shared?	The system provides payroll data to DoD for purposes of completing the payroll process.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	<p>The following reports may be produced on individuals:</p> <ul style="list-style-type: none"> • Employee information (name, team, tour of duty) • Uncertified employees • Employees with Missing time • Team/Roster Listing of timekeepers and certifiers • Retroactive Data Uncertified Employees • Add • SAL_BEN • DANGERPAY • MANPOWER • RECON • 453 Error Report
15. What will be the use of these reports?	Timekeepers, Certifiers, and other select individuals are granted access to these reports in order to ensure the accuracy of time and attendance data. Reports are not available to the general public.
16. Who will have access to these reports?	Timekeepers, Certifiers, and other employees or contractors whose job functions require access to this information.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	System audit logs are maintained to record system activity and Administrator activity for limited security purposes to ensure the integrity of the system.
18. What kinds of information are collected as a function of the monitoring of individuals?	<p>For security purposes, system audit logs are maintained to record system activity and Administrator activity. This activity includes invalid logon attempts and access and modification to data in the system.</p> <p>The Operating System/Server logs maintained by the EITS environment contains IP information; this is separate from the application/database logging specific to DPP.</p>



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Department of Energy Payroll Processing (DPP)

MODULE II – PII SYSTEMS & PROJECTS

19. Are controls implemented to prevent unauthorized monitoring of individuals?	DPP has established policies and procedures for controlling and monitoring access to the system. These are defined in the Security Plan and are compliant with privacy controls in NIST 800-53, rev 4.
--	--

DATA MANAGEMENT & MAINTENANCE

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.	The accuracy of the data in the system is verified at the close of every pay period (every two weeks) by authorized DOE system administration staff.
--	--

21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The system is only maintained at DOE HQ in the EITS DC&SS. Privileged access to the system is only available within DOENET using 2 factor authentication. The system operates in the Microsoft Azure Cloud.
---	---

Records Management

22. Identify the record(s).	Records relating to employee compensation such as time and attendance records. The Department of Energy Payroll Processing (DPP) manages payroll services for the entire U.S. Department of Energy (DOE).
------------------------------------	--

23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Employee Compensation and Benefits Records: GRS 2.4, item 030 Payroll program administrative records. Records produced in administering and operating payroll functions of a general nature and not linked to an individual employee's pay: GRS 2.4, item 60 and 61
---	--

24. Records Contact	Sean Kennedy Sean.Kennedy@hq.doe.gov 240-315-6772
----------------------------	---

ACCESS, SAFEGUARDS & SECURITY



PRIVACY IMPACT ASSESSMENT
 Office of Chief Financial Officer
 Department of Energy Payroll Processing (DPP)

MODULE II – PII SYSTEMS & PROJECTS

<p>25. What controls are in place to protect the data from unauthorized access, modification or use?</p>	<p>Through the Office of the Chief Financial Officer’s (CF) Assessment and Accreditation program and annual assessment processes, all baseline security controls have been implemented and tested as appropriate to its Federal Information Processing (FIPS) categorization in accordance with the Senior DOE Management Program Cyber Security Plan (PCSP) and DOE Directives. The system was certified and accredited with full Authority To Operate and found to have mitigated risk to an acceptable level.</p> <p>Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access via Role Based Access Controls (RBAC) and Single Sign On (SSO) leveraging OneID integration. These access controls are defined in the system security plan. All system team members (Federal and contractor) are required to take the DOE standard cyber security certification course as a prerequisite for the system access. Data encryption is involved with DPP, per the System Security Plan.</p> <p>Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include non-disclosure agreements, role-based access so individuals only have access to appropriate personal information, and use of system audit logs to monitor access and user activity in the system.</p>
<p>26. Who will have access to PII data?</p>	<p>DOE Federal and contractor personnel with authorized access to DOE networks will have access to their own data in the system. Access to others’ PII will be strictly controlled based on job responsibility and function. System Administrators and help desk staff will have access to all data in the system. Payroll personnel have access to data for those individuals they are responsible to administer.</p>
<p>27. How is access to PII data determined?</p>	<p>System Access control lists are established to allow System Administrators access to only view and change data for which they are responsible. Payroll personnel have access to data for those individuals they are responsible to administer.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>Yes, the system provides data to the Defense Civilian Pay System (DCPS) for purposes of completing the payroll process.</p>



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Department of Energy Payroll Processing (DPP)

MODULE II – PII SYSTEMS & PROJECTS

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?

There is an Interconnection Security Agreement (ISA) with Defense Finance & Accounting Service (DFAS) and a Data Interface Agreement (DIA) with Bonneville Power Administration (BPA).

30. Who is responsible for ensuring the authorized use of personal information?

System Owner, the Chief Financial Officer, and the Director for Corporate Business Systems.

END OF MODULE II



PRIVACY IMPACT ASSESSMENT
Office of Chief Financial Officer
Department of Energy Payroll Processing (DPP)

SIGNATURE PAGE		
	Signature	Date
System Owner	<p>Logan Kwedar</p> <hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
Local Privacy Act Officer	<p>Ana Manchester</p> <hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
Chief Privacy Officer	<p>William K. Hunt</p> <hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>