USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed "Gender" and "Sexual Orientation" from Biographical Information in accordance with Executive Order 14168, "Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government."

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	BMC Helix – Cloud Services (BMC Helix – CS)
Program Office	OCIO
Mission Area	CEC
CSAM Number	2094
Date Submitted for Review	04.7.2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Hugh Woolard	Hugh.woolard@usda.gov	816-926-3446
Information System Security Manager	Robert Lee	Rob.lee@usda.gov	910-431-8634
System/Program Managers	Isaac White	Isaac.white@usda.gov	240-446-8178

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

This Privacy Impact Assessment (PIA) addresses the BMC Helix Cloud Service (BMC HELIX-CS) of Governance Services Division (GSD). BMC HELIX-CS is a SAAS, Software as a Service, cloud offered by BMC which provides a comprehensive service management suite for its customers. This PIA is being conducted based on the results of the Privacy Threshold Analysis (PTA) OCIO Client Technology Services (CEC) Governance Services Division (GSD) which indicated that a PIA was required.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

BMC Helix Cloud Service (BMC HELIX-CS) is a SAAS tool implemented to centralize various functions for information technology. Some of these functions include service desk workflow, self-service ticketing, change management, problem management, knowledge management, and asset management.

BMC HELIX provides the following functionality:

- A full set of IT service management (ITSM) modules that share native, purpose built architecture.
- Embedded best-practice process flows.
- A closed loop change & release process tied to incidents and problems.
- Self-Service request catalog for IT, Security, and Business needs.
- Tracking incident response times and service desk performance against SLAs.
- Real-time Performance and ROI metrics reporting.
- Ability to track asset CIs in a robust CMDB backend.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

Collection of information by USDA personnel will be governed by the Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Guidance can be found in Appendix III to 0MB Circular No. A-130 and NIST SP-800-30, Risk Management Guide for Information Technology Systems.

1.2. Has Authorization and Accreditation (A&A) been completed for the system?

BMC Helix – Cloud Services (BMC Helix – CS) Approved 012025.

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

The exact mechanism may be slightly different for each government client. Notice is provided during the new account request process. The user must acknowledge the informed consent provisions with a signature during the new account request process. This was presented in November of 2015, and it was determined that a SORN was not required for this system.

1.4. Is the collection of information covered by the Paperwork Reduction Act?

No

Section 2: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers

☐ Social Security number	☐ Truncated or Partial Social Security number	☐ Driver's License number
☐ Passport number	☐ License Plate number	☐ Registration number
☐ File/Case ID number	☐ Student ID number	☐ Federal Student Aid number
☐ Employee Identification number	☐ Alien Registration number	☐ DOD ID number
☐ Professional License number	☐ Taxpayer Identification number	☐ Business Taxpayer Identification number (sole proprietor)
☐ Credit/Debit Card number	☐ Business Credit Card number (sole proprietor)	☐ Vehicle Identification number
☐ Business Vehicle Identification number (sole proprietor)	☐ Personal Bank Account number	☐ Business Bank Account number (sole proprietor)
☐ Personal Device Identifiers or Serial numbers	☐ Business Device Identifiers or Serial numbers (sole proprietor)	☐ Personal Mobile number

☐ Health Plan Beneficiary number
☐ Business Mobile number (sole proprietor)
☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)
☐ Business Mailing Address (sole proprietor)
☐ Date of Birth (MM/DD/YY)

☐ Ethnicity
☐ Business Phone or Fax Number (sole proprietor)
☐ Country of Birth

☐ City or County of Birth
☐ Group Organization/Membership
☐ Religion/Religious Preference

☐ Citizenship
☐ Immigration Status
☐ Home Phone or Fax Number

☒ Home Address
☒ ZIP Code
☐ Marital Status

☐ Spouse Information
☐ Children Information
☐ Military Service Information

☐ Race
☐ Nationality
☐ Mother's Maiden Name

☐ Personal Email Address
☐ Business Email Address
☐ Global Positioning System (GPS)/Location Data

☐ Employment Information
☐ Alias (Username/Screenname)
☐ Personal Financial Information (Including loan information)

☐ Education Information
☐ Resume or Curriculum Vitae
☐ Business Financial Information (Including loan information)

☐ Professional/Personal References

Biometrics

☐ Fingerprints
☐ Hair Color
☐ DNA Sample or Profile

☐ Retina/Iris Scans
☐ Video Recording

Distinguishing Features

☐ Palm Prints	☐ Eye Color	☐ Signatures
☐ Dental Profile	☐ Photos	

Characteristics

☐ Vascular Scans	☐ Height	☐ Weight
☐ Scars, Marks, Tattoos	☐ Voice/Audio Recording	

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)	☐ Cell Tower Records (e.g., Logs, User Location, Time)	☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information	☐ Mental Health Information	☐ Disability Information
☐ Workers' Compensation Information	☐ Patient ID Number	☐ Emergency Contact Information

Specific Information/File Types

☐ Personnel Files	☐ Law Enforcement Information	☐ Credit History Information
☐ Health Information	☐ Academic/Professional Background Information	☐ Civil/Criminal History Information/Police Record
☐ Case Files	☐ Security Clearance/Background Check	☐ Taxpayer Information/Tax Return Information

[List additional information collected but not listed above here (for example, a personal phone number that is used as a business number).]

2.2. What are the sources of the information in the system/program?

Information will be provided by USDA OCIO CEC administrators or USDA personnel that utilize the CEC BMC HELIX system. Some information is provided from other USDA systems of record. Privacy Impact Assessment – Remedy on Demand - CS Page 5 People records are originated and updated from our USDA HR records via a daily EEMS import. Some Site location data is created and updated from updates created in the NRCS OIP system. Some requests are created automatically by input from other systems, including JIRA, SCOM, HPOpenview, SolarWinds, Govminder, Control-M(RD), and Xerox.

2.2.1. How is the information collected?

Some of the Personnel information used by CEC BMC HELIX will be provided by USDA through the USDA EEMS/SailPoint system. Other information is provided through our Access Control process, input by Agency SAAR POCs during the input process of the specific access requests. Some information is automatically transferred from other systems as documented in Item 1.2 above.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

The only publicly available data used is the Zip Code Database from the US Postal Service. This is used for some agencies as site information, where specific Gov't Offices are unknown. The only data used is the Zip Code, City, County and State.

2.4. How will the information be checked for accuracy? How often will it be checked?

The accuracy of the data provided to BMC HELIX by USDA will be the responsibility of the data owner in most cases. BMC HELIX does provide some verification, at a data type layer (i.e., Numeric, Date, Text formats). BMC HELIX also can verify the accuracy of the information based on unique identifiers built within the system (i.e., GUIDs, Email Addresses, etc.), but only for updates to current records.

2.5. Does the system/program use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

This system does not use or interface with 3rd party websites.

2.5.1.1. What PII will be made available to the agency though the use of third-party websites?

None

2.6. **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: By implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

Section 3: Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

BMC HELIX stores and leverages data in support of a robust IT Service Management (ITSM) application. The data can include people data (i.e., Names, Office Site Info, Organizational info, contact information, etc.), incident requests, change requests, problem tickets, knowledge base articles, and hardware assets.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

Access controls are in place to protect the information system and its components. All systems will be segmented by the public and secured or hardened following Fed Ramp Moderate guidance.

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Mitigation: By Implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

The exact mechanism may be slightly different for each government client. Typically, the agency employee, contractor, or stakeholder does not have the opportunity to decline to provide non-PII information. The information requested is required to assign and set up the user accounts. The user has the right to correct or update information at any time be sending an email request to the agency help desk.

4.2. What options are available for individuals to consent, decline, or opt out of the project?

The exact mechanism may be slightly different for each government client. Generally, the requirement is for each account to be uniquely tied to an individual, all other information may be changed, updated or deleted by sending an email request to the agency help desk.

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: **Privacy Act risks associated with notices include:**

Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Non-compliance with Regulations: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

User Consent: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Section 5: Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?

Information will be maintained if users are actively using the system. If a user leaves USDA and no longer requires access. Personnel from USDA will be required to disable and then remove the account as required.

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Per USDA, this system now qualifies as an electronic record keeping system. Records will be maintained in accordance with the guidelines defined by the Client (US Government Agency that contracts for the use of the system).

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: Data is retained on users as they actively use the system, therefore the account information is required until the user no longer needs access. The active management of accounts will enable USDA to remove personnel that no longer require access and account management features provide additional security including the ability to change passwords or re-create accounts if needed for security reasons. Request Records continue to identify Basic User information (Name, Site location), even after the User record has been deleted. This ensures accurate reporting for all ITSM Requests. Records are maintained for 3 years within the active Remedy system and then automatically archived and maintained on an Archive server. So, no Request record is ever deleted.

Mitigation: Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Shared with USDA-FPAC ServiceNow system, to transfer ticket data for internal USDA FBC support customers.

Shared with USDA-MRP ServiceNow system, to transfer ticket data for internal USDA MRP Support of customer.

Share with 1OCIO Dashboards (Tableau System), for purposes of Reporting to USDA Management.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: **Privacy risks associated with internal sharing and disclosure include:**

Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

Data Breaches: Internal systems can be vulnerable to breaches, compromising PII.

Insider Threats: Employees with malicious intent may exploit their access to PII for personal gain.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Access Controls: Implement role-based access controls to limit who can access PII based on their job responsibilities.

Encryption: Use encryption for data in transit and at rest to protect PII from unauthorized access.

Regular Training: Provide ongoing training for employees on data privacy policies, the importance of protecting PII, and how to handle it securely.

With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

None

6.3. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: **Privacy risks associated with external sharing and disclosure include:**

Unauthorized Access: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Data Breaches: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Loss of Control: Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Data Sharing Policy: Develop a clear policy outlining the conditions under which PII can be shared externally, including legal and compliance requirements (ex.: Computer Matching Agreements, SORNs, Business Agreements).

Due Diligence: Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.

Written Agreements: Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.

Section 7: Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1. What are the procedures that allow individuals to gain access to their information?

The owner of data is responsible for classifying their data based on Federal guidelines. If an owner is unknown for a data asset, the OCIO-CEC or the client organization's ISSM, Information System Security Manager, becomes its caretaker. Each ISSM is responsible for developing, implementing, and maintaining procedures for identifying all data assets and the associated owners. Personnel information will be available for their review using the Remedy People form maintained by USDA. The user may view their information by going into Remedy, select the "My Profile" option. Once in their People record, the user will see their detailed information.

7.2. What are the procedures for correcting inaccurate or erroneous information?

The data owner/user has the right to correct or update information at any time.

7.3. How are individuals notified of the procedures for correcting their information?

During the new user request process, users are informed of their right to correct or update information at any time.

7.4. If no formal redress is provided, what alternatives are available to the individual?

The user has the right to correct or update information at any time.

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

Privacy Risk: Privacy Act risks associated with redress include:

Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Failure to Address Complaints: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

Mitigation: By implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

Dedicated Privacy Officer/Privacy Point of Contact: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

Section 8: Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

8.1. How is the information in the system/project/program secured?

The CEC BMC HELIX system uses the baseline moderate impact security controls from NIST SP 800-53 Revision 4 in establishing security mechanisms to protect the system. This includes border protection, auditing and alerting for tracking and monitoring events on the system.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

Access to the system will be limited to administrative personnel in support of the service. The CEC BMC HELIX system details which groups have access to the various components of the system based on their relevant roles.

8.3. How does the program review and approve information sharing requirements?

By having data transmitted to and stored at an additional facility the risk is increased, however the use of encryption decreases the potential compromise of data. This risk may be reduced further by USDA by limiting the private information that gets stored and using file level encryption for sensitive data.

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

OCIO CEC provides security and awareness training to personnel managing the CEC BMC HELIX system for employees/contractors on an annual basis. Security training is required during the onboarding process of all users added to the BMC HELIX system. A security background check is also required for all users' priors being added to the BMC HELIX system.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 5/28/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.07.02 03:17:58 -04'00'

Signed:_____

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed:_____

Issac White
Information System Owner
USDA-OCIO-CEC
U.S. Department of Agriculture

Signed:_____

Hugh Woolard
Mission Area Privacy Officer
USDA-OCIO-CEC
U.S. Department of Agriculture