

Privacy Impact Assessment

Name of System: OpsPlanner Version 3.3

System's Unique ID: OpsPlanner

SYSTEM APPLICATION/GENERAL INFORMATION:

1. What is the purpose of the system/application?

The OpsPlanner application is an integrated Continuity of Operations (COOP), Incident Management, and Automated Notification software tool that enables users to collaborate, create, plan, and manage NARA's emergency and disaster prevention, preparedness, notification, response and recovery practices and procedures in one comprehensive, all hazards emergency management system via the web and using one tool.

Federal departments and agencies must have plans in place that will ensure they can continue to conduct their essential operations, and provide essential services, following a disaster or other emergency that disrupts normal operations. In the federal government, this planning discipline can be referred to as Continuity of Operations (COOP), emergency planning, or disaster recovery (DR) planning. All of these terms describe aspects of the planning effort NARA must take to ensure that it can fulfill its mission following any emergency.

Organizations, such as NARA, that operate many facilities over a wide geographic area, face challenges in the creation and management of such plans. These planning activities require a significant amount of collaboration, the collection and management of large amounts of documents and other data, the ability to notify all staff quickly in an emergency, and the ability to regain control of the organization to manage it through any crisis. Without a specialized set of tools to assist with this planning and response effort, NARA may face an uncertain future after a disaster.

While the very nature of emergency planning involves some measure of uncertainty, this can be mitigated given an unlimited budget for emergency planning/response staff, or an automated tool to assist with these planning/response activities.

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

- (a) 44 USC - US Code - Title 44: Public Printing and Documents (January 2003)
- (b) Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, November 18, 1988, (as amended by Executive Order 13286, *Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security*, 28 February 2003). Assigns national security emergency preparedness responsibilities to Federal departments and agencies. Under this order, agencies are required to have capabilities to meet essential defense and civilian needs during any national security emergency. The head of each agency shall provide for: 1) succession to office and emergency delegation of authority in accordance with applicable law; 2) safekeeping of essential resources, facilities, and records; and, 3) establishment of emergency operating facilities.

- (c) National Security Presidential Directive/NSPD-51 and Homeland Security Presidential Directive/HSPD-20, National Continuity Policy, May 9, 2009. Requires Federal agencies to have in place a comprehensive and effective program to ensure survival of our constitutional form of government and continuity of essential Federal functions under all circumstances
- (d) Federal Continuity Directive (FCD) 1, Federal Executive Branch Continuity Program, February 14, 2008. The Federal Emergency Management Agency, under authority established in NSPD-51/HSPD-20, published FCD 1 to outline the steps federal executive departments and agencies will follow to ensure the continuity of their essential functions and to return to normal operations following any disruption. FCD 1 details the process to determine essential functions, as well as the elements of a federal COOP plan.

DATA in the SYSTEM

1. Describe the information (data elements and fields) available in the system in the following categories:

a. Employees

- (1) **Users** (A user is any employee who is given access rights to the system data.)
 - E-mail – Required. The e-mail address of the new user.
 - Last Name – Required. The last name of the new user. The system will accept a maximum of 30 characters in any alpha/numeric or special character combination with the exception of ‘&’.
 - First Name – Required. The first name of the new user. The system will accept a maximum of 30 characters in any alpha/numeric or special character combination with the exception of ‘&’.
 - Job Title – Optional. The job title of the new user.
 - Business Phone – Required. This is the business phone number for the new user.
 - Cell Phone – Required. This is the cell phone number for the new user.
 - Home Phone – Required. This is the home phone number for the new user.
 - Fax - Optional. The fax number of the new user.
 - Pager - Optional. The pager number of the new user.
 - Address 1 – Optional. The first line of the street address of the new user.
 - Address 2 – Optional. The second line of the street address of the new user.
 - City - Optional. The city of the new user.
 - State - Optional. The state of the new user.
 - Zip Code - Optional. The postal code or zip code of the new user.
 - Notes – Optional. Additional notes pertinent to the new user.
- (2) **Contacts** (A contact is any employee, volunteer, intern, contractor or others, who needs to be reached during an emergency, including system users.)
 - Organization – Required if Contact Last Name or Contact First Name is not used. The name of the organization to which the new contact belongs.
 - Contact Last Name - Required if Organization Contact First name is not used. The last name of the new contact.

- Contact First Name - Required if Organization or Contact Last Name is not used. The first name of the new contact.
- Business Phone 1 – Required. The main phone number for the new contact.
- Business Phone 2 – Optional. An additional phone number for the new contact.
- Business Phone 3 – Optional. An additional phone number for the new contact.
- Fax - Optional. The fax number for the new contact.
- Pager - Optional. The pager number for the new contact.
- E-mail - Optional. The e-mail address for the new contact.
- Category – Required. The category of the new contact.
- Street Address 1 – Optional. The first line of the street address of the new contact.
- Street Address 2 – Optional. The second line of the street address of the new contact.
- City - Optional. The city of the new contact.
- State - Optional. The state of the new contact.
- Postal Code - Optional. The postal code or zip code of the new contact.
- Country - Optional. The country of the new contact.
- Notes – Optional. Additional notes pertinent to the new contact.

b. External Users: None planned, although NARA may at its option include external users such as other government agencies, local police and fire, media organizations, etc. for notification purposes only.

c. Audit trail information (including employee log-in information):

OpsPlanner™ captures important actions that can be reviewed and analyzed to determine applicable post-analysis plan improvement or for audit reviews following the events. Audit entries are time-stamped by the system. Events are captured in the following categories:

- Security Success (including login): Events in the system that were attempted, and were successful. For example, an administrator might want to know who has been accessing the system. A report can be run on user logins that provides this information. The report pulls information from the Security Success audit log.
- Security Failure (including login): Events in the system that were attempted, and were not successful. For example, an administrator might want to know who has been trying to access the system without proper credentials. A report can be run on user logins that provides this information. The report pulls information from the Security Failure audit log.
- Error: Used only by OpsPlanner™ developers. Designates very severe error events that will presumably lead the application to abort.
- Information: Used only by OpsPlanner™ developers. Designates informational messages that highlight the progress of application components.
- Warning: Used only by OpsPlanner™ developers. Designates potentially harmful situations that could impact application performance.
- Debug: Used only by OpsPlanner™ developers. Designates fine-grained informational events that are most useful to debug an application. Debug is turned off by default and enabled only when needed to diagnose a specific application issue.

For each of the above categories, the following data elements are captured:

- **Event ID:** 1

- **Type:** Security Failure Audit
- **Date:** 01/23/2007
- **Time:** 10:08:24 AM
- **User:** System User
- **Category:** General
- **Event Title:** User Login
- **Message Description:** User: xxx@nara.gov from IP:xxx.xxx.172.216 could not be authenticated against database
- **Source:** OpWatch.OpsPlanner.Web.Admin.UserControl.LoginCredentials

d. Other (describe):

OpsPlanner™ is organized in a hierarchical structure that reflects NARA's locations, organizational units, and plan types. Plans are customizable to NARA's specific business needs, but may include:

- **Occupant emergency plans (OEP):** Describe the specific measures NARA staff, contractors, and visitors will take to respond to a facility emergency. These could include evacuate (leave the building) or shelter-in-place (go to a safe area in the building) plans.
- **Salvage plans:** Describe the steps NARA staff or authorized contractors will take to limit and, where possible, reverse damage to NARA-managed record. Records can be electronic (e.g.: a scanned photograph) or traditional (e.g.: The Bill of Rights.)
- **Continuity of Operations (COOP) plans:** Describe the measures that NARA has taken to continue mission-essential functions and services following any emergency.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

a. NARA operational records:

NARA operational records will be included as necessary to support NARA's COOP and disaster recovery capability. Some examples of operational records that may be necessary to support this system may include personnel records, financing and budget records, and property management files. These may be included in the OpsPlanner database in their current form or may be integrated into NARA's OpsPlanner-based plans.

b. External users:

If NARA chooses to use the OpsPlanner notification engine to make contact with external users following an emergency, these users would need to provide their names and sufficient contact information as described above.

c. Employees:

See Sec 1.a.(1) and .(2) above.

d. Other Federal agencies (list agency):

None at this time.

e. State and local agencies (list agency):

None at this time.

f. Other third party source:

None at this time.

3. Is each data element required for the business purpose of the system? Explain.

The business purpose of the system is to facilitate NARA's emergency planning and response activities. As discussed above, this requires sufficient planning elements and procedural/operational detail, as well as contact information for those who will be contacted through the OpsPlanner notification engine.

4. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.). The data will be collected from individuals through use of a NARA collection form. The data will be validated at least quarterly through testing and exercising for accuracy per NARA's COOP plan.

5. Is there another source for the data? Explain how that source is or is not used?

No.

ATTRIBUTES OF THE DATA

1. 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.

2. Will the new data be placed in the individual's record? No, as the system does not derive new data or create previously unavailable data about individuals.

3. Can the system make determinations about employees/public that would not be possible without the new data? No, as the system does not derive new data or create previously unavailable data about individuals.

4. How will the new data be verified for relevance and accuracy? Not applicable, as the system does not derive new data or create previously unavailable data about individuals.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Data in OpsPlanner is only accessible using an assigned login id and password. In addition, users will only have access to view the data of individuals to whom they have been assigned management duties over. Only the System Administrator will have access to all data held in the system. Further, audit function capabilities are enabled in the system, whereby all access to the system data can be monitored.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain. Processes are not being consolidated.

7. Generally, how will the data be retrieved by the user? All users will log in to the application and establish a secure SSL connection. SSL is a data encryption protocol which provides secure communications over the Internet.

8. If the data is retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual. Yes. User/contact data can be retrieved through a name search. Search can be conducted on first and/or last name.

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

OpsPlanner includes the following reports by default:

- Contacts - by Location
- Contacts - by Organizational Unit
- Contacts - by Plan Type
- Contacts - by Category and List
- Deleted Users (standard)
- Plan Team Members - by Location
- Plan Team Members - by Organizational Unit
- Plan Team Members - by Plan Type
- User Group's Access Privileges
- User's Access Privileges
- Users' Last Login

Only authorized system administrators designated by NARA will have access to these reports. These reports are used for the administration of the tool and to centrally manage planning activities. Reports can only be accessed by authorized individuals designated by NARA.

The only persons who will have access to the OpsPlanner Master Contact List are those who have been granted Contact List Manager permissions by the System Administrator. The persons granted Contact List Manager permissions are the Emergency and Continuity Plan Owners and Planners responsible for developing their plan(s) and/or insuring that they are executed in the event of an emergency. Office Points of Contact (POC's) who will be gathering the contact information for their individual offices and employees will not have access to the OpsPlanner Master Contact list unless they are Planners who have been granted Contact List Manager Permissions. Access to the Master Contact List is required for Planners to select and build the contact lists that are applicable to the plans for which they are responsible.

10. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent? Provision of information in the system is voluntary and will not be used for purposes other than those authorized for the system. Employees will be requested to provide their data for collection in OpsPlanner for emergency instances where they may need to be contacted. However, employees are not obligated to provide their information. The collection form will inform employees that if they choose not to have their information included in OpsPlanner then NARA may not have the ability to contact them should an emergency arise.

11. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not applicable, as the system does not make or support the making of negative determinations of any nature.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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? The system uses full dual-site redundancy between San Antonio, TX and Reston, VA. Consistent use of the system and data are maintained through SQL database replication.

2. What are the retention periods for records in this system? Records that contain PII data elements are currently unscheduled and therefore not authorized to be destroyed. NASS is working with NH at NARA to develop new dispositions.

3. What are the procedures for disposition of the records at the end of the retention period? Only Emergency Planning records are currently scheduled and will be disposed of in accordance with files no. 235 through 239 (Emergency Planning) of Files 203. Records that contain PII data elements are currently unscheduled. Records that are currently unscheduled including all records related to actual emergency and contingency events and related operational files, and the emergency management contact and notification records that contain PII data elements will not be destroyed or disposed of until the Archivist approves an SF 115, Request for Records Disposition Authority. These records will be retained until the NARA Records Officer provides approved disposition instructions. NASS is working with NH at NARA to develop new dispositions.

4. How long will the reports produced be kept?

Emergency Planning Reports reflecting agency-wide results of tests will be permanently retained in accordance with disposition instructions for files no. 238. Reports accumulating from tests conducted under NARA emergency plans excluding consolidated and comprehensive reports under file no. 238 will be destroyed when 3 years old in accordance with disposition instructions for file no 239.

5. Where are the procedures documented?

NARA Files 203

6. Cite the disposition instructions for records that have an approved records disposition in accordance with FILES 203.

See above

7. If the records are unscheduled they cannot be destroyed or purged until the schedule is approved.

See above

8. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe. No.

9. How does the use of this technology affect public/employee privacy? N/A

10. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established. Explain. Yes.

OpsPlanner implements user login and passwords to monitor the access capability of users and captures audit trail information, including Security Success' such as events in the system that were attempted and were successful, and Security Failures when events are attempted and are unsuccessful.

11. What kinds of information is collected as a function of the monitoring of individuals?

No information is collected through monitoring activities, as stated above.

12. What controls will be used to prevent unauthorized monitoring? The system is not capable of monitoring, but access to the system by unauthorized users is controlled through SSL encryption, user passwords, and system security audit reviews. Access to all data in OpsPlanner is permission based and limited only to those users with a need to know that specific information. Users only have access to those plans and data for which they have been granted permission by the System Administrator or Plan Owners. The OpsPlanner has a systems log that tracks all user access to the system and maintains those logs for at least 90 days.

13. Can the use of the system allow NARA to treat the public, employees or other differently? If yes, explain. No.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors? No.

15. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

- NARA 12 - Emergency Notification Files

16. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain. Yes, NARA 12 will be amended.

ACCESS TO DATA

1. Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, other). NARA system administrators and Paradigm contractors, at NARA's discretion.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Access to the data is determined by NARA's emergency planning and response staff. Access is determined on a "need-to-know" basis and is limited to strict business need. Specific procedures will be documented in a NARA Standard Operating Procedure (SOP), currently under development.

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

Explain. User access is restricted based on the following role-based permissions:

- **Announcement Creator:** This role allows a User to create, modify, or delete their own public or internal announcements. However, this User can only view other announcements created by other Users.

- **Announcements Administrator:** This role allows a User to view, create, modify, or delete any public or internal Announcement.
- **Contact Categories Administrator:** This role allows a User to view, create, rename, or delete any Contact Category.
- **Contact List Administrator:** This role allows a User to view, create, modify, or delete any Contact List.
- **Contact List Creator:** This role allows a User to view, create, modify, or delete their own Contact List(s).
- **Dependency Administrator:** This role allows a User to view, create, modify, and delete Dependency Category and Items.
- **Dependency Creator:** This role allows a User to view, create, modify, and delete Dependency Items.
- **Dependency Viewer:** This role allows a User to view Dependency Items.
- **Event Manager:** This role allows a User to declare, modify, and view all Events in the Recover module.
- **License Manager:** This role allows a User to update OpsPlanner License information with the assistance of a Paradigm TAC representative.
- **Locations Administrator:** This role allows a User to view, create, modify, and delete Locations.
- **Organization Unit Administrator:** This role allows a User to view, create, modify, and delete Organizational Units.
- **Plan Types Administrator:** This role allows a User to view, create, modify, and delete Plan Types.
- **Planning Administrator:** This role allows a User to view, create, modify, or delete any Plan document within OpsPlanner regardless of individual Plan Ownership, Plan Permissions, or Team Membership.
- **Reports Administrator:** This role allows a User to upload, modify, view, or delete any OpsPlanner report.
- **Resource Catalog Administrator:** This role allows a User to view, create, modify, and delete Resource Catalog Items.
- **Survey Creator:** This role allows a User to view, create, modify, or delete their own Survey(s).
- **Surveys Administrator:** This role allows a User to view, create, modify, or delete any survey.
- **System Log Viewer:** This role allows a User to view and run the System Log.
- **Task Creator:** This role allows a User to view, create, modify, or delete their own Collaboration Task(s).
- **Tasks Administrator:** This role allows a User to view, create, modify, or delete any Collaboration Task.
- **User Groups Administrator:** This role allows a User to view, create, modify, or delete any User Group.
- **Users Administrator:** This role allows a User to view, create, modify, or delete any User.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access? (Please list processes and training materials).
 Through the permissions detailed above, user access will be restricted only to a users own data or

data for which he/she would have normal access as defined/authorized by the COOP Program Manager.

Source documents (i.e. Excel Spreadsheets) will list the names and provide the data cells the POC's will use to gather the employee contact information and return it to the OpsPlanner Systems Administrator. These source documents will only contain data for the personnel in the office of section for which the POC is responsible. The source documents will contain the data previously gathered and on file for the persons in that particular office or section so the POC can periodically verify and update the information. POC's will only have access to the data relating to those individuals for whom they are responsible.

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Yes, contractors will be involved with system maintenance. Yes, appropriate Privacy Act contract clauses were included in the contracts.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. No.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment? N/A

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? NARA's Senior Agency Official for Privacy and the Product Owner/COOP Program Manager.

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency, state how the data will be used and the official responsible for proper use of the data. No.

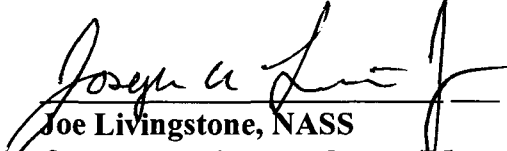
See Attached Approval Page

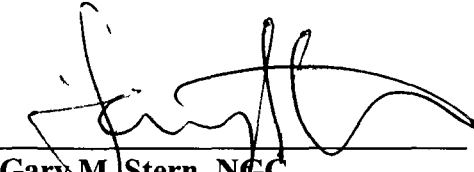
Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

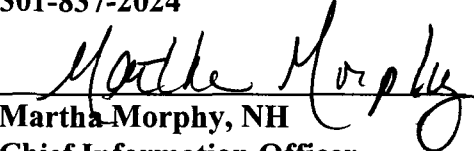
IT Security Manager

Privacy Act Officer

The Following Officials Have Approved this PIA

 (Signature) 09/14/09 (Date)
Joe Livingstone, NASS
OpsPlanner System Owner/Manager
8601 Adelphi Road
College Park, Maryland 20740

 (Signature) 9/21/09 (Date)
Gary M. Stern, NCC
Senior Agency Official for Privacy
8601 Adelphi Rd, Room 3110
College Park, MD
301-837-2024

 (Signature) 9/21/09 (Date)
Martha Morphy, NH
Chief Information Officer
8601 Adelphi Rd, Room 4400
College Park, MD
301-837-1992