Privacy Impact Assessment for

Document Approval System Hub (DASH)

November 24, 2020

Contact Point

Steve Hickman
Deputy Executive Secretary
Office of the Director

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The Document Approval System Hub (DASH) is a web-based application designed to electronically store, access, and route documents through the U.S. Office of Personnel Management's (OPM) internal clearance process. DASH is used throughout OPM to circulate and communicate about a wide range of documents that require coordination and approval. These documents include, among others, internal and external policies; responses to Congressional letters; reports to Congress or other agencies; proposed and final regulations for publication in the Federal Register; and responses to letters from current or former Federal employees, annuitants, and members of the public. This Privacy Impact Assessment (PIA) is being conducted because certain of the documents and communications within the system associated with those documents may contain personally identifiable information (PII).

Overview

The Document Approval System Hub (DASH) is a web-based application designed to electronically store, access, and route documents through the U.S. Office of Personnel Management's (OPM) internal clearance process. DASH is owned by the Office of the Executive Secretariat (ExecSec) in the Office of the Director (OD) and is used throughout OPM to circulate and communicate about a wide range of documents that require coordination and approval. These documents include, among others, internal and external policies; responses to Congressional letters; reports to Congress or other agencies; proposed and final regulations for publication in the Federal Register; final agency decisions related to EEO complaints; and correspondence from and in response to current or former Federal employees, annuitants, and members of the public. DASH takes advantage of the content management and document routing components available in Salesforce, a cloud-based Platform-as-a-Service (PaaS). Salesforce provides a platform for developing and/or purchasing third-party custom applications as well as a high degree of integration with Microsoft Office products, which enables DASH to use Outlook email and Active Directory in its processes. The Salesforce platform enables the DASH document management solution for the agency to store, access, manage and support the flow of documents through the internal clearance process used by OPM and managed by ExecSec.

DASH primarily uses the concept of a “Package” to compile and collect information needed to coordinate and manage the flow of documents through the review and approval process. The Package includes the document or documents to be approved, any related requests pertaining to the documents, the routing list of those who need to review and their assigned tasks, and all communications and decisions regarding the documents as they move through the review and approval process.

All DASH users are assigned one or more roles within a program office for interacting with Packages. These roles include Intake Specialist, Driver, Reviewer, Approver, Super Driver, and Administrator.

Intake Specialists create a Package using the Intake Screen in DASH. In doing so, they identify the subject of the Package, provide a summary description, and assign the Package a category, a due date, and a priority level. They have the option to immediately route the Package to a Driver or hold onto it until enough information can be ascertained, including identifying the proper Program Office. The Intake Specialist may upload documents for review and editing by others. Once the Intake Specialist fills out the mandatory fields on the Package Details Screen, they can route the package to the applicable Program Office. The Intake Specialist assigns the Package to the responsible Driver. At this point, the Intake Specialist has no further work to do on the Package until the Package completes its routing. Once the Package completes its routing, the Driver may route the package back to the Intake Specialist, who closes the package. Not all Packages will begin with an Intake Specialist; generally, this role will be assigned to an individual who is responsible for routing correspondence or other communications from outside of OPM to the appropriate Program Office for handling.

A Driver acts as the Package Manager within a Program Office. Drivers can create a Package just as an Intake Specialist can, or they can receive a Package from an Intake Specialist. It is the Driver’s responsibility to create a Routing List to achieve the required reviews and approvals. The Driver is also responsible for setting a Package’s priority, placing Packages on hold, and adding weigh-ins to a Package. The Driver is responsible for knowing the office’s standard operating procedures for who must review a package and is able to set up a Contacts list of other DASH users within DASH for ease of reference in creating Routing Lists. Once the Package has been saved and the workflow started, DASH uses the Routing List to alert the first individual on the list that they have been assigned a task on a Package. System alerts are sent using a Simple Mail Transfer Protocol (SMTP) hosted by Microsoft Office 365. As each user completes the assigned task, DASH updates the Routing List and alerts the next individual. This process continues until all actions on the Routing List have been completed. The Driver reviews the final document(s) and closes the Package in accordance with standard operating procedures. As the Package moves through the Routing List, the Driver is able to monitor progress and receive communication from other users about the Package. Only those on the applicable Routing List for the Package, or those who have been added as the Package circulates, are able to view the Package and edit the documents within.

Reviewers have permissions to view and edit all documents embedded in a Package that is assigned to them from a Driver. Some offices may have multiple Reviewers within their own program area prior to their Driver moving the Package to other Reviewers in other offices. When a Reviewer receives the Package, they open the package and review the attached documents. They may edit the documents or embed comments and once complete, upload the new version into the Package in DASH for movement to the next person on the Routing List. When a Reviewer uploads a new version of a document, DASH will request that they identify all changes. A Reviewer may use the Chatter function within DASH to send a message to another DASH user to ask questions, request additional information, or provide awareness regarding the Package. Chatter messages are viewable within DASH to all users on the Routing List with permissions to access a particular Package. The Reviewer may also use the Share function within DASH to share the Package with another DASH user who is not on the Routing List but who the Reviewer determines has a need to know. Through the Share function, additional DASH users may be provided read-only access or read/write access. The request to share is directed to the Driver who then provides the Package to the additional user.

The Approvers' primary role is to approve the completed documents within a Package. Just like Reviewers, they can view and edit all the documents associated with the routing activities they are assigned to. If they Approve the content of the Package, they document their approval for the Package to move on. If they are not ready to approve the package, Approvers can reject with comments indicating what needs to be changed or recommending who in other offices should review the Package before it can proceed. Drivers and Reviewers may also be Approvers.

Super Drivers are the those within each Program Office who need to track and ensure packages are being completed on time. Super Drivers can access all Packages in their Program Office to delegate roles, approve or review. Only the Super Driver in ExecSec and the Administrator in the Office of the Chief Information Officer (OCIO) has permissions to access all of the Packages within DASH.

Authorization and access to DASH is controlled by an Administrator who adds screened users to the appropriate directory and groups that can access DASH. The Office of the Chief Information Officer is the Administrator of DASH and has overall responsibility for maintaining the application. They create and maintain choice lists, user groups, user roles, offices, and other configurations at the request and direction of ExecSec, the owner of DASH.

The Administrator has permissions to access any user's account when troubleshooting at the request of the user.

Within DASH, all users have the ability to use the Search function to find a Package in the system using any data criteria stored in DASH, including Package information, activity information, and user information. Only those Packages that the particular user has permission to access, however, will be returned. In addition, all users will be presented with a personal Dashboard when they log into DASH. The dashboard will provide them with summary information concerning the Packages and tasks within those Packages for which they are responsible.

Many of the Packages in DASH will contain minimal information about individuals, such as the contact information for those OPM personnel who are connected to the Package. Some Packages, however, contain more significant and sensitive personally identifiable information (PII). For example, DASH may be used to circulate incoming correspondence and responses about an individual's retirement benefits or health care coverage. In addition, final agency decisions regarding Equal Employment Opportunity cases will also route through DASH for review and approval. Users of DASH will be trained to recognize PII in Packages, to minimize the amount of PII that they include in communications about the Package within DASH, where possible to redact PII if it is not necessary to include, and to limit the Routing Lists for Packages that contain sensitive information, including sensitive PII, to only those who have a need to know the information.

Reports within DASH can be generated by Super-Drivers and Drivers for their program areas, and can be based on any field within the Package. In addition, Administrators can generate OPM-wide Reports. All users can access these reports, but within each Report will only see those entries related to Packages for which they have permission-based access. A Printable View/EDS of each Package is also available and provides a view of the Package, to include the title, summary, synopsis of approval, and other per-determined fields established within DASH.

DASH does not share any information with other systems within OPM, or outside of OPM. All system users with a need-to-know must authenticate to Microsoft Office 365, Salesforce online, and DASH by using their existing user account information from the Active Directory in Microsoft Office 365. Security authentications are also enforced within the application.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The documents contained in DASH are compiled subject to the various authorities pertaining to OPM's program offices as well as pursuant to the authority of the Director under 5 U.S.C. 302(b) and 5 U.S.C. 1103(a) and are routed for clearance and approval based on OPM's Reservations and Delegations of Program Authority, and OPM's Reservations and Delegations of Administrative Authority.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

In general, records in DASH are not retrieved by an individual's name or other personal identifier and, accordingly, are not subject to the Privacy Act. Those records in DASH that are or may be retrieved by an individual's name or identifier include, for example, certain correspondence as well as EEO final agency decisions. Those records may be subject to OPM Internal 21, Correspondence Management, EEOC/Gov't 1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Records, or other SORN applicable to the specific subject matter of the record.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

There is a Security System Plan for DASH currently under executive review. DASH is presently operating under an Interim Authority to Test (IATT) for six months.   The system will undergo a security assessment and authorization review by the end of 2020, with the expectation that this will result in an Authorization to Operate (ATO).

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

These records contained in DASH will be maintained under schedule DAA-0478-2017-0002.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The Paperwork Reduction Act does not apply to DASH; DASH does not collect information directly from members of the public.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

DASH is designed to electronically collect, store, access, and route documents through OPM's internal clearance process. These documents include, among others, internal and external policies; responses to Congressional letters; reports to Congress, the White House, or other agencies; proposed and final regulations for publication in the Federal Register; Paperwork Reduction Act information collections; communications materials; responses to letters from current or former Federal employees, annuitants, and members of the public; and EEO final agency decisions. In addition to the documents themselves, the DASH system contains comments, messages, and decisions by those OPM personnel who are responsible for compiling, reviewing, and/or approving a particular DASH Package.

Within the DASH Packages, documents and communications may include information about individuals, including contact information for internal OPM personnel and names, mailing addresses, phone numbers, email addresses, retirement claim numbers, and other information about an individual included in correspondence with OPM or necessary for inclusion in documenting an OPM decision (such as with EEO final agency decisions).

2.2. What are the sources of the information and how is the information collected for the project?

Authorized and authenticated DASH users within OPM program offices are responsible for creating packages within DASH to coordinate the internal review and approval of documents. Information in the packages comes from a wide variety of sources, such as OPM personnel responsible for drafting regulations, policies, reports, and other documents, current and former Federal employees and members of the public who correspond with OPM, Members of Congress seeking information, or policy drafts from OPM management and DASH users who comment, send message, revise documents, and record decisions about particular DASH Packages within the system.

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

No, DASH does not use information from commercial sources or publicly available data.

2.4. Discuss how accuracy of the data is ensured.

DASH users are responsible for reviewing the accuracy of the information contained within a DASH Package before it is routed to the next person on the Routing List and to provide comment and revisions regarding any information that they find to be inaccurate. In particular Intake Specialists and Drivers are responsible for including all relevant documents in a Package for review.

DASH users will ultimately have access to a training manual, standard operating procedures, and a guide containing best practices in order to address the accuracy of information in DASH.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that more information than is necessary will be included in DASH, including unnecessary personally identifiable information.

Mitigation: This risk is mitigated through training DASH users on what information is required to be included for routing DASH Packages and on identifying and redacting any unnecessary PII when creating and reviewing/approving a Package. In addition, certain sensitive documents containing PII, such as HR-related documents and contracts are, by policy and practice, not routed for review and approval within DASH.

Privacy Risk: There is a risk that the information in DASH is not accurate and will result in an erroneous decision.

Mitigation: This risk is mitigated through training DASH users to review and provide revisions and comments on any information that is not accurate. With respect to information about individuals that comes from sources outside of OPM, it is not possible to fully ensure accuracy and certain PII that is obtained, for example, directly from an individual or through another source on behalf of an individual is presumed to be accurate.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The information in DASH is used to circulate and communicate about a wide range of documents that require coordination and approval within OPM.

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

No, DASH does not use technology in order to discover or locate predictive patterns and anomalies.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

There are authorized DASH users in every program office in OPM, to include Drivers, Super Drivers, Reviewers, and Approvers. Routing lists for specific DASH Packages determine which users in the various program offices will have access to the Package and any requests to add additional people to the Routing List are sent to the Driver for consideration. Each program office has a Super User who has access to all Packages assigned to or initiating from the program, and ExecSec has a Super User who has access to all packages, as does the Administrator within OCIO for troubleshooting purposes.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the information about individuals contained in DASH may be accessed and used by an unauthorized person or by an authorized person for an unauthorized purpose.

Mitigation: This risk is mitigated by the establishment of specific user roles within the system, limiting access to specific Packages to only those with a need to know. In addition, only those users who are designated on the Routing List for a specific package will have access to the Package. This risk is further mitigated through appropriate training of the various DASH users and via publication of standard operating procedures.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Individuals whose information may be included in DASH Packages and who are not OPM users of DASH do not interact with the system and are not provided notice that their information may be used and maintained within DASH. DASH is used solely by OPM users within the boundaries of OPM. To the extent any of the information included in DASH is obtained directly from individuals at the original point of collection, appropriate notice should be provided at that time. In addition, notice concerning certain records is provide in any applicable Privacy Act system of records notice and notice concerning DASH and the records contained therein is provided through publication of this PIA.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals whose information may be included in DASH Packages and who are not OPM users of DASH do not interact with the system and are not provided notice that their information may be used and maintained within DASH, nor are they provided with the opportunity to opt out of their information being included in DASH. DASH is used solely by OPM users within the boundaries of OPM. To the extent any of the information included in DASH is obtained directly from individuals at the original point of collection, appropriate notice and opportunity to consent, decline to provide, or opt out should be provided at that time. Those individuals who submit correspondence to OPM either directly or via Congress do so voluntarily and implicitly consent to OPM’s review and response.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not have notice that their information is included in DASH and will not be able to consent to, decline, or opt out of including their information.

Mitigation: This risk is not mitigated directly by DASH but is appropriately mitigated via the publication of this PIA and through appropriate communication with the individual at the point at which their information is collected outside of the system.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

All of the records in DASH are subject to records schedule DAA-0478-2017-0002 and are treated as permanent records and will be transferred to NARA after 15 years.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the records in DASH will be retained for longer than is necessary.

Mitigation: This risk is not fully mitigated. While the majority of the records in DASH are permanent, there may be a small percentage that could more properly be retained for a shorter period of time. Through discussions with NARA and considering the overall risk associated with longer than necessary retention, it was determined that all records in DASH will be treated under the same schedule. As DASH develops and evolves, ExecSec will re-examine this with the Agency Records Office and NARA.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

DASH is OPM’s tool for internal clearance and review. Some of the documents within DASH Packages, such as policies, Government-wide memos, and communications documents, are ultimately shared with the public as part of normal agency operations. However, they are not shared directly from DASH as the system is not designed to share externally.

Responses to correspondence are not shared outside of OPM other than to provide a response to the individual correspondent.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

In general, records in DASH are not retrieved by an individual's name or other personal identifier and, accordingly, are not subject to the Privacy Act. Those records in DASH that are or may be retrieved by an individual's name or identifier and as such are subject to the Privacy Act will only be shared consistent with the purpose and routine uses in the applicable SORN.

6.3. Does the project place limitations on re-dissemination?

To the extent documents in DASH are shared externally as described in Section 6.1, OPM does not generally place any limitations on their re-dissemination.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

DASH is not specifically designed for external sharing and as such does not maintain records of disclosures within the system. Any applicable requirement to maintain such records will generally be done outside of DASH; but DASH is subject to auditing and an Administrator can ascertain when and by whom documents may be accessed and downloaded from the system.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in DASH will be shared externally for a purpose other than that for which it was originally generated and maintained.

Mitigation: This risk is mitigated in that DASH is not designed for direct external sharing and is further mitigated by limiting access to the document sin DASH to only those with a need to know and training those DASH users who have access to and the ability to download documents from DASH in the appropriate handling of that information.

Section 7.0. Redress

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

Individuals whose information is contained within DASH Packages do not have direct access to DASH and the documents contained therein. To the extent that DASH contains records about an individual that are subject to the Privacy Act (e.g., correspondence, see Section 1.2), the applicable system of records notice provides information regarding the process for obtaining access to those records. To the extent records are not covered by the Privacy Act, individuals may request access to agency records via the Freedom of Information Act (FOIA). See https://www.opm.gov/information-management/freedom-of-information-act/.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals whose information is contained within DASH Packages do not have direct access to DASH and the documents contained therein. To the extent that DASH contains records about an individual that are subject to the Privacy Act (e.g., correspondence, see Section 1.2), the applicable system of records notice provides information regarding the process for obtaining access and requesting amendment to those records.

7.3. How does the project notify individuals about the procedures for correcting their information?

Individuals whose information is contained within DASH Packages do not have direct access to DASH and the documents contained therein and therefore DASH does not provide any notification to individuals. To the extent that DASH contains records about an individual that are subject to the Privacy Act (e.g., correspondence, see Section 1.2), the applicable system of records notice provides information regarding the process for obtaining access to and requesting amendment of those records.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not have access to or the ability to request amendment of records about themselves that are contained in DASH.

Mitigation: This risk is mitigated for those records that are subject to the Privacy Act by providing information to individuals via the applicable SORN. To the extent DASH records are not subject to the Privacy Act, the FOIA is available for individuals to request appropriate access to agency records.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

All DASH users are trained regarding the appropriate use of the system and hold designated user roles with varying levels of responsibility. For example, the Driver of a particular Package is charged with developing a Routing List that includes only those individuals who have a need to know and review/approve a Package. The Driver monitors access to the Package an Reviewers and Approvers are responsible for only communicating about a Package with others in the system who have a need to know its contents. DASH contains extensive audit logs that are reviewed by the Administrator and system owner regularly to provide overall monitoring of DASH on a regular basis.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees are required to receive annual Security and Privacy Awareness training. In addition, all DASH users will receive training on appropriate DASH use, standard operating procedures, and addressing PII within DASH. DASH users receive role-based training that covers the how to identify PII and what types of PII should be redacted in before uploading documents and comments into DASH.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

System access to DASH is controlled by the DASH Administrator. DASH access requests are approved by the various programs and submitted to the DASH Administrator, who is responsible for adding user(s) to the appropriate Active Directory and Groups with the appropriate access and role designation within DASH.

Access to individual packages and associated attachments is controlled by Drivers who create the Routing List for a particular Package; only individuals that appear on the Routing List for a particular Package can access it.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

DASH does not share information outside of the system and does not require information sharing agreements. Any new uses for the system or the information contained therein will be reviewed by ExecSec and appropriate OPM stakeholders, as necessary.

Responsible Officials

Steve Hickman
Deputy Executive Secretary
Office of the Director

Approval Signature

Signed Copy on file with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer