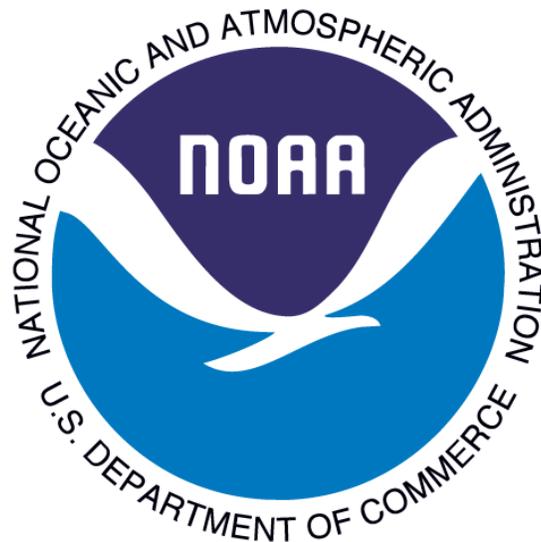


**U. S. Department of Commerce
National Oceanic and Atmospheric Administration**



**Unified Messaging System (UMS)
NOAA0301**

PRIVACY IMPACT ASSESSMENT

June 2012

Prepared by: Sarah D. Brabson, Stefan Leeb, Sandra Giger, Tommy Thompson, Ernest Maravilla

Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

*Property of the United States Government
For Official Use Only*

Name-of-System: Unified Messaging System

Unique Project Identifier: 006-48-02-00-01-3511-00

IT Security System: NOAA0301

Description: NOAA's Unified Messaging System is our contract for Google Apps for Government (GAfG). Google Apps services include electronic mail, calendar synchronized with email, office productivity (document creation and management, mostly using documents, spreadsheets, and presentations, but also diagrams, video, and geo-referenced data) and internal Web site hosting.

Google, Inc. hosts Google Apps services via its remote Web servers, and stores data in remote Google Data Centers. The user has availability of services and data virtually via Internet connections known as the "cloud" or "cloud computing", and the user is no longer running the IT services in-house as was done previously.

The NOAA UMS completed its migration of the NOAA legacy email and calendar services, and users' online email files, calendar information, and contacts to the GAfG cloud on December 12, 2011. UMS receives, routes, and retain NOAA's email through the GAfG cloud. The GAfG applications are offered collectively as a service. The applications work in coordination with established NOAA services (e.g., Lightweight Directory Access Protocol (LDAP), and NOAA interfaces, e.g., Outlook and Thunderbird.

Google Mail Services use Internet Message Access Protocol over SSL (IMAPS) as a protocol for communicating with other NOAA mail clients. Each of the supported clients has full capability to receive, view, organize, sort, manage, delete, respond, and create emails. The mailbox capacity of 25GB ensures that users can keep larger amounts of email for active work and for historic needs. The service utilizes Google's built-in search capabilities, so that these large mail stores can be queried for needed information. Servers that support the UMS/Google solution reside in a redundant, highly available, backed-up, online storage environment. This provides a better long-term retention capability than current local mail stores which put mail at risk of loss. UMS, through Google Apps, provides a calendar function that is closely tied to the mail system. Calendaring and email work in tandem facilitating scheduling, communication, and resource allocation. The UMS also receives email address and LDAP account updates from the NOAA Message Operations Center (MOC). However, the UMS does not interconnect with or ingest additional data/information from other NOAA organizations, federal agencies or commercial entities.

Additional GAfG services include Docs, Sites and Video. These applications are designed for sharing of information with, and collaboration with, designated individuals or groups. The owner of the Doc, Site, or Video chooses to whom it is available, for reading/viewing, or for reading and editing.

*Property of the United States Government
For Official Use Only*

1. What information is to be collected (e.g., nature and source)?

The UMS transmits, processes, and stores email sent through or to the noaa.gov domain. General information that is transmitted both internally and externally through email is used for the communication of work related activities such as project responsibilities, program documents, and other artifacts, etc. However, NOAA anticipates that some information such as names, date of birth, home address, business location, etc. may appear in emails.

The UMS does not specifically intend to collect and store Personally Identifiable Information (PII), yet some of the email that is sent or received may contain PII. Google will retain email that may contain records subject to the Privacy Act. However, it is against NOAA policy to include PII in emails. The email may contain information that is subject to the Privacy Act. Files or attachments sent via email containing PII are required to be encrypted in accordance with NOAA policy – most recently addressed in a February 4, 2010 Memorandum from the NOAA CIO, Protecting Personally Identifiable Information (PII), as well as the [DOC Electronic Transmission of Personally Identifiable Information \(PII\) Policy](#). Google encrypts all emails, but only during transit, and this does not include attachments.

Sensitive business information, e.g. pre-decisional documents, is also not included in emails but if attached to an email, should be encrypted. Google Docs and Sites are also not intended to contain PII or sensitive business information, and information available through these applications is also covered by the DOC policy.

2. Why is the information being collected (e.g., to determine eligibility)?

All information that is sent by email is at the discretion of the sender. The user determines what emails, files, and attachments he/she wants to keep. Information in Google Docs or on Google Sites is used for the purposes for which the Doc or Site was created: general information or information shared with specific colleagues, working groups or committees for the purposes of accomplishing tasks or making decisions.

In some specific cases, only at the direction of authorized NOAA representatives, information from the various products which comprise GAfG may be aggregated and made available to authorized individual(s) for purposes such as FOIA requests, litigation, Congressional inquiry, etc.

Federal agencies conducting “the distribution and performance of its” business through such means as email, calendar, Docs, Sites and Videos are authorized by [5 U.S.C. 301: Government Organization and Employees, Departmental Regulations](#). NOAA’s undertaking the Unified Messaging System/GAfG is part of its Strategic IT Plan for FY2012-16 and aligns with the Office of Management and Budget’s (OMB’s) 25-Point Implementation Plan to Reform Federal Information Technology Management – which recommends that the application of “light technology” and shared solutions, including

shifting to a “Cloud First” policy – by providing a common Cloud-based platform for email, calendar, collaboration and information sharing.

3. What is the intended use of the information (e.g., to verify existing data)?

The Google Apps suite integrates messaging with cloud-base business productivity software services in order to create and share messages, calendars, text documents, forms and spreadsheets, presentations, diagrams, videos, and collaborative websites for internal use. Information sent through email or made available through the Calendar, Docs and Sites is used for conducting business and/or to provide general information within NOAA.

Google hosts Mail and Google Message Discovery (GMD) from its Data Centers in the Continental United States (CONUS). Google, outside of UMS, does not analyze or make decisions regarding individual email activity.

GMD provides email security and a centralized, searchable repository to locate email quickly in the event of legal discovery (e.g., collecting an individual mailbox for an Inspector General (IG) investigation, or a FOIA request) or a security investigation.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

Once an email, the email content, and attached files are processed and stored by Google, the received data will not be shared with any other organization outside of NOAA, except as directed or required by an appropriately authorized individual or organization.

Google will maintain the ‘filing cabinet’ and will not access the contents other than the minimum required to maintain the UMS system. A Google employee, who supports multiple Google Apps customers in the Google cloud (for example, Google Data Center system administrators, Google Enterprise support staff and engineers), is authorized to support UMS upon request by [NOAA] UMS Administrators for Tier-3 Customer Service and troubleshooting.

Only designated NOAA staff members (i.e. certain UMS Administrators) will be authorized to perform the aggregation for FOIA and similar requests. (A UMS Administrator is someone who is supporting UMS and NOAA directly.)

Inspecting users’ email is done via the GMD. Unless a UMS Administrators is granted specific authentication credentials to access the GMD, then he/she cannot access or view users’ Google Mail messages. Although the UMS administrators see GAfG account information via the C-Panel interface, the C-Panel does not contain user-created data (such as email or documents).

Following Standard Operating Procedure (SOP), at the direction of authorized NOAA representatives, information from the various products that comprise GAfG may be aggregated and made available to authorized individual(s) for purposes such as FOIA requests, litigation, Congressional inquiry, etc.

Regarding Calendar, a UMS Administrator *with “super Admin”* privilege may view, and reconfigure the settings for users’ calendars in the GAFG noaa.gov domain (“super Admin privilege” is the most trusted permission to do everything possible, globally, in UMS.)

Google Docs (presently in transition to be known as “Drive”), and Sites files are shared with specific people, whom the owner and/or editors invite by name or group to share. Usage of Sites is subject to comprehensive guidance pending from OCIO, including the prohibition to store PII in GAFG.

Regarding Docs, the UMS Administrator normally has no ability to see, link to, download, or access any Google Docs file, or collection of files, unless either: (1) the owner of the file(s) gives explicit permission to a named noaa.gov account or group of accounts that includes the UMS Administrator; (2) the UMS Administrator files a problem ticket with Google Enterprise Support to request a fix to a problem; or (3) a UMS Administrator *with super admin privileges* uses C-Panel to transfer ownership of all the Docs from one user to another user account (and although transferring ownership, still cannot view the data).

Regarding Sites, a UMS Administrator *with super Admin* privileges may not only visit and view any Site in noaa.gov, but is able to perform all the same actions as a Site “Owner”, including configuration, design, and deletion. However, if a Site has embedded Google Docs, the visibility of those Google Documents is still constrained by unique and separate document permissions that were configured by the document owner.

5. 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 may individual grant consent?

All NOAA personnel and support contractors are assigned a NOAA email account. The mandatory NOAA Security Awareness Training course contains a module titled “email Use and Security” that addresses risks, appropriate use, and privacy and monitoring expectations associated with NOAA email. All personnel are required to complete this training annually. NOAA email users understand that they are not to include PII or sensitive BII in emails and that any information that is put in email or email attachments can be viewed by designated and authorized NOAA personnel.

Docs, Sites or Videos are developed by/shared with a designated group of NOAA staff. They are not intended to contain PII or sensitive business information.

6. How will the information be secured (e.g., administrative and technological controls)?

National Institute of Standards and Technology Special Publication 800-53 (NIST-800-53), Recommended Security Controls for Federal Information Systems and Organizations, August 2009, identifies security controls for high, low, and moderate impact systems.

The UMS risk impact is based on, and the system is identified to have, a “MODERATE” Security Categorization, as depicted in the Federal Information Processing Standard Publication 199, Standards for the Security Categorization of Federal Information and Information Systems, *February 2004*.

UMS has selected a set of security controls for the information system based on the moderate impact level and minimum security requirements defined in FIPS 200; apply tailoring guidance; supplement the tailored baseline security controls based on NOAA’s assessment of risk and conditions including environment of operation, organization specific security requirements, specific threat information, cost-benefit analyses, special circumstances; and specific assurance requirements.

Security control assurance is implemented within UMS and obtained by actions taken by developers, implementers, and operators in the specification, design, development, implementation, operation, and maintenance of security controls; and actions taken by security control assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. For security controls in moderate-impact systems the emphasis is on increasing the grounds for confidence in control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific capabilities to increase grounds for confidence that the control meets its function or purpose.

An Authorization to Operate (ATO) under the [Federal Information Security Act of 2002](#) (FISMA), was awarded on December 9, 2011. The Assessment & Authorization (A&A) process is part of the NOAA Risk Management Framework (RMF) Process that continuously monitors policies, procedures, as well as, management, operational, and technical security controls required for all federal government IT systems. NOAA’s RMF program also includes rigorous continuous monitoring integrated into the system development life cycle. The objective of the continuous monitoring program is to determine if the set of deployed security controls continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the environment. NOAA’s RMF is a well designed and well-managed continuous monitoring program that effectively transforms an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of UMS.

The following controls are relevant to protecting privacy data that may be collected by the UMS.

Management Controls:

*Property of the United States Government
For Official Use Only*

All UMS personnel undergo a national agency check with inquiries (NACI) security check when employed or contracted. This involves a check of federal and local law enforcement records to ensure the trustworthiness of the employee.

Operational Controls:

Google Systems Administrators, UMS Google Apps (CPANEL) Administrators, and UMS Help Desk personnel are trained regarding the secure operations and maintenance of the UMS. The NOAA user community has access to training regarding the proper use of the available Google applications.

UMS will maintain a virtual operating environment within the Google Data Centers in CONUS for GAfG email. Content referenced in a Google Doc is solely hosted in CONUS. The protection of media associated with these two entities is covered by contract. Google practices configuration management across its global deployment to update its services, after thorough testing outside of the noaa.gov GAfG domain to ensure proper operation and to mitigate vulnerabilities. Antivirus and intrusion detection capabilities monitor for malicious activities. Some of Google data centers may be in European Union countries which may slightly decrease the privacy and security of data stored there. However, exclusion or encryption of PII per NOAA policy and FISMA A&A compliance, and exclusion of procurement-sensitive, budget or pre-decisional information should significantly mitigate this risk.

Physical and environmental controls are in place within the Terramark facility and the Google processing environment. These controls meet or exceed NIST and NOAA requirements. The UMS has developed and implemented a NOAA UMS Incident Response Plan (IRP) that is aligned with and interfaces with the NOAA-Computer Incident Response capability, as well as those with Google and Terremark.

Technical Controls:

Google network Intrusion Detection Systems and firewall ensure that the UMS is not accessed by an unauthorized source. Customer information is encrypted except when it is needed and being used by a customer service employee, who accesses the information using an encrypted connection.

Two-factor authentication is required for administrative and privileged access to the UMS support services hosted at Terremark. Remote administration of the servers is performed over encrypted channels, and only approved administrators that have authorized access to the servers are allowed to log in. Server backups are performed continually. Only approved Google Data Center system administrators (NOT USERS) or authorized engineers have access to Google servers. Access to core Google services is not extended to other personnel in Google or NOAA. Authorized UMS and NOAA APPS C-Panel admin accounts only maintain the virtual C-Panel dashboard user interface. They are not granted administrative rights to the actual servers.

All Google Apps data (including email, documents, and sites) is encrypted (HTTPS) during transmission between the Google Apps for Government cloud and the user. Data at rest that is stored in Google Data Centers, although non-encrypted per the FIPS standard, is stored using a method that makes it unreadable without other security keys spanning access across several servers.

The principle of least access is applied for access to all resources. The system provides for user roles assigned by administrative staff. A written protocol for authorizing, managing, and logging access is part of the system development. Changes to the system will be tracked and recorded through a strict change control process.

Data Extract Logging and Verification:

UMS does not generate extracts of emails, privacy information, or sensitive data unless so directed by an official NOAA or DOC order. Email or privacy data would not be extracted to other sources (i.e., printouts, reports, etc).

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

No. The PII that may be contained in the email records that NOAA0301 uses is covered by a variety of existing NOAA, Department of Commerce, and Government-wide systems of records. The information system does not create a new system of records, but instead may store or use data subject to other system of records notices. See the Federal Register's [2011 Compilation](#) of Privacy Act issuances for NOAA's SORNs. Docs and Sites do not contain PII.

8. Are these records covered by an approved records control schedule?

The UMS does not change the current "print and file" policy that an email message, including attachments, that is a record must be printed out and filed in the case folder or with the other correspondence to which it relates. This ensures that the documentation of a case, transaction, or other activity is maintained in a comprehensive and readily retrievable manner. The email messages in the UMS are not a substitute for the official paper files. The [NOAA Records Management Handbook](#), item 200-12 - Electronic Mail Records held in an Email System, provides that "electronic mail messages that meet the definition of Federal records, and any attachments to the record messages AFTER they have been printed and filed in paper form, copied to an electronic record keeping system, or scanned for record keeping purposes," have the authorized disposition, "Delete from the email system after copying to a record keeping system."

The UMS retains the history of NOAA email and email attachments in the Google Message Discovery archive. For active user accounts, sent and received email are online until deleted by the account; owned and shared Docs and Sites are online until deleted by the owner(s) or transferred to other accounts. Regarding Docs and Sites, NOAA record

retention schedules of offices generating them would apply (reference [NOAA Record Schedules](#)).