Lorraine Robidoux - NOAA Federal <lorraine.robidoux@noaa.gov>

Improved Means to Protect Sensitive Information

1 message

CIO Announcements <cio.announcement@noaa.gov> Mon, Apr 6, 2020 at 1:54 PM
To: _BCAST NOAA All Hands <bcast-noaa-all@noaa.gov>
Cc: cpurvis@doc.gov, Mark Graff - NOAA Federal <mark.graff@noaa.gov>, Adrienne Thomas - NOAA Federal <adrienne.thomas@noaa.gov>

Message From the Chief Information Officer

April 6, 2020

MEMORANDUM FOR: All NOAA IT Users, Including Contractors and Affiliates

FROM: Zachary Goldstein
Chief Information Officer and Director, High Performance Computing and Communications
National Oceanic and Atmospheric Administration

SUBJECT: Improved Means to Protect Sensitive Information

NOAA is now making additional tools available for storing and transmitting sensitive data within the Google Environment, as well as easing access to the Kiteworks tool. The purpose of this Memorandum is to notify users that they will now be allowed to store and transmit Sensitive, non-public information within Google Drive and Gmail, provided that that information is not shared with anyone outside of the noaa.gov domain. Additionally, Kiteworks continues to be an acceptable alternative for the transmission and storage of Sensitive PII, both internal and external to the noaa.gov domain. Kiteworks is now available via Common Access Card (CAC) single sign-on (SSO). To access Kiteworks via SSO, click on the link “Login via the external SSO provider” on the Kiteworks landing page https://sfc.doc.gov/#/folder/0 .

NOAA’s reliance on technological solutions for communication and collaboration has led to an unprecedented capability to carry out its mission anywhere, anytime. This mission—which directly protects United States citizens’ lives and safety—frequently requires the collection, use, and storage of sensitive information, including personally identifiable information (PII) and business identifiable information (BII).

One subset of PII includes data that, if released, could cause harm or identity loss to the individual, such as social security numbers, passport numbers, dates of birth, and other sensitive personal data. This Sensitive PII, as well as all BII, requires special handling, controls, and protections in its storage and transmission. We must be particularly aware of these protections during this time of increased telework.

NOAA's enterprise use of the Google suite allows for real-time collaboration, innovative work solutions, and leverages an unlimited email storage capability. However, the Google platform's encryption capabilities, which are needed to protect Sensitive PII and BII, have limitations, and therefore, constraints on their use.

Constraints on transmitting or storing Sensitive PII or BII in Google to avoid committing a privacy violation:

1. Users must never send Sensitive PII or BII by Gmail if any recipient is outside of the noaa.gov domain, and no Sensitive PII should ever be sent using a personal email platform. All recipients' email addresses or Google Drive link-sharing addresses must end in noaa.gov; otherwise, any transmission of Sensitive PII—even with other Bureaus in the Department or other agencies in the Federal Government—violates the DOC Electronic Transmission of PII Policy.
2. Neither Google nor Kiteworks should ever be used to transmit sensitive PII or BII to a group box. Kiteworks is still an acceptable encrypted platform for folder-sharing of Sensitive PII and BII.
3. Any Google Drive folders that store Sensitive PII or BII must have link sharing off, and must not be shared with users outside of the noaa.gov domain. Additionally users must select the following options in the advanced settings: Prevent editors from changing access and adding new people, and, Disable options to download, print, and copy for commenters and viewers.
4. It is the sender's responsibility to ensure that all recipients of Sensitive PII or BII, whether by email or Google Drive link, are authorized to have access to the data and have a need-to-know.
5. Users should still abide by Privacy best practices, including limiting Sensitive PII or BII storage overall where possible, avoiding accessing Sensitive PII from personal devices (such as sending, retrieving, or storing copies of an SF-50s from a personal device), and avoid the use, collection, transmission, or storage of Social Security numbers if the Commerce Department's Senior Agency Official for Privacy has not concurred with the applicable Privacy Impact Assessment.
6. Users who store sensitive or non-public data--for example, PII or BII--within Drive are required to indicate the nature of the data within the title of the Drive folder so that users can properly handle and limit the distribution of that data.

Conclusion

By using Google's offerings for the storage and transmission of sensitive information, including sensitive PII and BII, we will directly improve our ability to prevent, monitor, detect, and respond to Privacy incidents, and we will improve our role as stewards of the sensitive data we maintain. If you have questions or concerns, please contact the UMS Helpdesk, or contact Mark Graff, NOAA BCPO, at mark.graff@noaa.gov. Additional training and information regarding appropriate use of NOAA IT resources can be found in the IT Security Awareness Training.

Thank you all for securing NOAA's sensitive data assets by properly employing this technology when transmitting and storing the PII and BII entrusted to NOAA in carrying out our important mission.

Regards,
Zach

Zachary G. Goldstein
Chief Information Officer and Director, High Performance Computing and Communications
National Oceanic and Atmospheric Administration