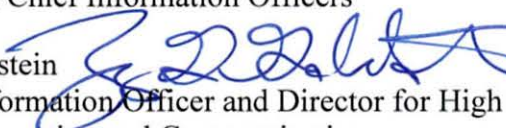




U.S. DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
Office of the Chief Information Officer
High Performance Computing and Communications
CHIEF INFORMATION OFFICER

August 28, 2017

MEMORANDUM FOR: NOAA Assistant Chief Information Officers

FROM: Zachary G. Goldstein 
NOAA Chief Information Officer and Director for High
Performance Computing and Communications

SUBJECT: Use of GitHub.com at NOAA

PURPOSE:

This memo authorizes staff at the National Oceanic and Atmospheric Administration to release select scientific products to GitHub.com public repositories. On August 8, 2016, the Office of Management and Budget (OMB) released M-16-21, "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software", which committed Federal agencies to using Open Source Software to better support cost efficiency, mission effectiveness, and the consumer experience with core Government programs. Git is an open-source version control system used for software development and GitHub is the web-based hosting service for the Git repository. NOAA's use of GitHub.com, in compliance with M-16-21, will enable NOAA scientists to not only collaborate more effectively with partners and researchers, but will also provide the general public with an increased level of accessibility to NOAA's research.

GitHub.com, however, is not considered a "trusted" collaboration environment by NOAA because there is no expectation of privacy or confidentiality for the information that is posted on GitHub.com, and the integrity and availability of information, once posted, cannot be assured. To address those issues, this memo serves as a definition of the type of content that is deemed acceptable for release into the GitHub environment, as well as my formal acceptance for the risks associated with posting of this information on GitHub.com.

ACCEPTABLE CONTENT

The following are the requirements that must be met before code, data, or documentation produced by NOAA staff can be released to GitHub.com:

- **Scientific Products:** The code, data, or documentation must be a scientific product, defined by the NOAA Scientific Integrity Policy (NAO 202-735D) as "Presentation of the results of scientific activities including the analysis, synthesis, compilation, or translation of scientific information and data into formats for the use of NOAA, the



Department of Commerce, or the Nation."

- *Associated Product risk*: The scientific product must be reasonably classifiable as FISMA Low, as outlined by the Federal Information Security Management Act of 2002. FISMA Low classification includes only information for which the unauthorized disclosure, unauthorized modification, unauthorized destruction, or disruption of access can be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. If the effect of such events would be **serious, severe, or catastrophic**, the information **cannot** be released under the authority of this memo.
- *No Controlled Unclassified Information (CUI)*: The information being released must not contain any sensitive data or information. NOAA staff must confirm that there are no account passwords, user logins, API keys, or other restricted information contained in the scientific product prior to releasing it to GitHub.com, through the use of the git-secrets scanning tool . Additionally, the information owner must confirm that there is no Personally Identifiable Information (PII) or Business Identifiable Information (BII) included with the content, nor any information that would allow access to PII or BII, they must also confirm that the data is not a CUI subcategory as listed at the following link: <https://www.archives.gov/cui>

POSTING REQUIREMENTS

The following are NOAA requirements and guidelines for posting NOAA content to public repositories:

- All NOAA generated content published externally on GitHub must also reside on a NOAA-controlled server within a NOAA boundary. This ensures that a "gold standard" copy of all content is maintained, to which only NOAA users have access. External submissions should be incorporated into the internal NOAA repository only after careful review and testing by the Information Owner and a scan by a NOAA GitHub Administrator.
- Information Owners should provide the GitHub Administrator the location of the data's gold standard for all of the repositories owned.
- All projects posted to the NOAAGov GitHub public repository must include a link to the location where the project code resides on the DOC or DOC bureau public website, as well as the following disclaimer in a README file:

"This repository is a scientific product and is not official communication of the National Oceanic and Atmospheric Administration, or the United States Department of Commerce. All NOAA GitHub project code is provided on an 'as is' basis and the user assumes responsibility for its use. Any claims against the Department of Commerce or Department of Commerce bureaus stemming from the use of this GitHub project will be governed by all applicable Federal law. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation or favoring by the Department of Commerce. The Department of Commerce seal and logo, or the seal and logo of a DOC bureau, shall not be used in any manner to imply endorsement of any commercial product or activity by DOC or the United States Government."

RISK MITIGATION

The following are the applicable NIST 800-53 standards, along with a description of the mitigations employed (including Information owner (IO) responsibilities), which reduce the residual risk to an acceptable level.

- *AC-20 - Use of External Systems: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to a) access the information system from the external information systems, and b) process, store, and/or transmit organization-controlled information using the external information systems.*

NOAA has established internal guidelines to ensure that users a) are aware of the risk to the confidentiality, integrity, and availability of the data, b) allow only appropriate information to be posted to GitHub.com, and c) provide write access only to authorized employees and contractors. Additionally, Information owners should develop and publish a clear guidance document for their collaborators, in order to communicate the restrictions of use and ensure appropriateness of GitHub.com activities. It is recommended that this guidance document be derived from the information contained in this memo and based on the Department of Commerce GitHub Guidance policy posted at <https://github.com/CommerceGov/Policies-and-Guidance/blob/master/GithubGuidanceforDepartmentofCommerce.md>. The guidance document should also contain any additional restrictions or guidance, as deemed appropriate by the IO.

- *AC-21 - Information Sharing: Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for the collaborative purpose.*

Semi-annual audits will be conducted by the IO to ensure only authorized collaborators have access to change the information.

- *AC-22 – Publicly Accessible Content: Designates individuals authorized to post information onto a publicly accessible information system.*

All information posted must be suitable for public release, as defined by this memo. It must also be reviewed prior to release through the use of the git-secrets scanning tool.

Additionally, the IO must authorize access for each user posting content, and must regularly review access procedures. The responsibilities of the IO include:

- Training authorized individuals to ensure that posted publicly-accessible information does not contain nonpublic information;
- Reviewing the proposed content of information prior to posting onto the publicly-accessible information system to ensure that nonpublic information is not included; and
- Reviewing the content on the publicly-accessible information system for

nonpublic information annually (or when updates are made), and removing such information and alerting the IT Security Officer, through a report to the NOAA Computer Incident Response Team, should such information be discovered.

- *SI-7 Software and Information integrity: The organization employs integrity verification tools to detect unauthorized changes to publicly available information.*

The IO ensures the integrity of the information posted on public sites by maintaining a copy within the NOAA system boundary. A controlled, “gold standard” version must be established prior to posting content to GitHub.com. This “gold standard” copy must be retained within the system boundary and controlled through the use of a NOAA-run version control tool such as an internally hosted Git server, which will be utilized to detect changes and provide version control.

- *SI-12 – Information Output Handling and Retention: The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.*

A copy of all information posted must be retained internally if it is no longer required for business use. Each IO may elect to retain information longer than this.