

Department of Commerce (DOC)
Office of the Chief Information Officer (OCIO)



Technical Review Package
For GitHub

Prepared by

Technical Review Board

Version 1.0

June 1, 2016

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

1. TRB RECOMMENDATION SUMMARY 2

1.1 ASSESSMENT SUMMARY2

1.2 RECOMMENDATION.....3

THE TECHNICAL REVIEW BOARD MET ON MAY 31, 2016 TO EVALUATE THE FINDINGS SUBMITTED BY THE SUBJECT MATTER EXPERTS IN THE FOLLOWING AREAS:.....3

2. APPENDIX OF TECHNICAL REVIEW FINDINGS 4

2.1 APPENDIX A – REQUEST FORM4

2.2 APPENDIX B – TERMS OF SERVICE5

2.3 APPENDIX C – USE CASE6

2.4 APPENDIX D – IT SECURITY REVIEW8

2.5 APPENDIX E – RECORDS MANAGEMENT10

2.6 APPENDIX F – SECTION 508 COMPLIANCE15

2.7 APPENDIX G – EA TRM16

2.8 APPENDIX H – PRIVACY17

1. TRB RECOMMENDATION SUMMARY

Product Name	GitHub	Product Web Site (url)	www.github.com		
Date	May 31, 2016				
Recommendation for Use	Approved	<input checked="" type="checkbox"/>	Not Approved	<input type="checkbox"/>	
TRB Lead	Tom Pennington, Chief EA		Email	tpennington@doc.gov	
TRB Lead Signature			Date		

1.1 Assessment Summary

OGC Terms of Service	Approved	<input checked="" type="checkbox"/>	Not Approved	<input type="checkbox"/>	N/A	<input type="checkbox"/>
IT Security Review	Approved	<input checked="" type="checkbox"/>	Not Approved	<input type="checkbox"/>	N/A	<input type="checkbox"/>
Records Management	Approved	<input checked="" type="checkbox"/>	Not Approved	<input type="checkbox"/>	N/A	<input type="checkbox"/>
Privacy	Approved	<input checked="" type="checkbox"/>	Not Approved	<input type="checkbox"/>	N/A	<input type="checkbox"/>
Section 508 Compliance	Approved	<input checked="" type="checkbox"/>	Not Approved	<input type="checkbox"/>	N/A	<input type="checkbox"/>
EA TRM	Approved	<input checked="" type="checkbox"/>	Not Approved	<input type="checkbox"/>	N/A	<input type="checkbox"/>

1.2 Recommendation

The Technical Review Board met on May 31, 2016 to evaluate the findings submitted by the subject matter experts in the following areas:

- OGC Terms of Service
- IT Security
- Records Management
- Privacy
- Section 508 Compliance
- Enterprise Architecture Technical Reference Model (EA TRM)

Based on these findings, the Enterprise Architects recommended the use of the free version of GitHub (www.github.com) to the Commerce Data Office (CDO) based on the use case submitted by the CDO. The use case can be found in the GitHub Technical Review Package in Appendix 3.

2. APPENDIX OF TECHNICAL REVIEW FINDINGS

2.1 Appendix A – Request Form

April 13, 2016

Product Name	Github	Product Web Site (url)	Github.com
Bureau	OS/ESA	Project Manager	
Requested By	Ian Kalin, Chief Data Officer	Supervisor	
Intended Users			
Number of Internal Users	>50	Number of External Users	N/A

Business/functional Need

[Describe the need and use of the product/service]

Open source collaboration to build software

Request Category (check all that apply)

Hardware	<input type="checkbox"/>	Software	<input type="checkbox"/>	Telecom	<input type="checkbox"/>	Website	<input type="checkbox"/>	Application	<input type="checkbox"/>
Other (Explain)	<input checked="" type="checkbox"/>	Cloud based software repository and social media tool							

Primary Business Drivers for Request

Policy Compliance	<input type="checkbox"/>	Legislative Compliance	<input type="checkbox"/>	Operating Plan Impact	<input type="checkbox"/>	IT Refresh	<input type="checkbox"/>	Business Improvement	<input type="checkbox"/>
Other: Explain	<input checked="" type="checkbox"/>	Used government-wide for open software development							

Details

	YES	NO
Will Department data be stored using this system/service?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Will PII or BII be accessed with this system/service?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Will this system/service be publicly accessible?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Will this system/service collect information from the public?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Approved by:		Date		For Office of the Chief Information Officer
--------------	--	------	--	---

2.2 Appendix B – Terms of Service

From: Grunstra, Lydia
Sent: Wednesday, April 03, 2013 11:04 AM
To: Kruger, Mike
Cc: Packard, Elise
Subject: GitHub TOS

Hi Mike,

This responds to your request for our office to review the updated Terms of Service (TOS) for GitHub, a free online code repository and code sharing site. Our office reviewed a prior iteration of GitHub's TOS on August 17, 2012. At that time, we advised that DOC could use GitHub after both parties signed an addendum created by the General Services Administration (GSA) to make the GitHub TOS appropriate for a Government agency. Recently, GitHub has updated their TOS. Although the updated TOS contains indemnification and state law provisions, which would otherwise be problematic, those provisions are nullified by the addendum that the parties signed in 2012. Accordingly, we see no legal concerns with DOC's continued use of GitHub.

Please let me know if you have any questions.

Best,

Lydia Grunstra
Attorney-Advisor
General Law Division
U.S. Department of Commerce
(202) 482-6113
lgrunstra@doc.gov

2.3 Appendix C – Use Case

Technology Request

TECHNOLOGY NAME:	Github.
BUSINESS OBJECTIVE:	Collaboratively build open-source software.
URL:	Github.com
POINT OF CONTACT:	Ian Kalin, Chief Data Officer
SUBMISSION DATE:	August 2015
REVISION DATE:	May 19 th , 2016

Planned Uses

The following table identifies how the requested technology will be used by the organization.

#	USE CASE
1	Collaboratively build open source software.
2	
3	
...n	

The following sections provide additional information regarding each proposed use.

Use Case #1

USE CASE:	<i>Collaboratively build open source software</i>
DESCRIPTION:	Revision control of code.
USERS(S):	30+ members of the Commerce Data Service.
STEPS:	The following provides a detailed listing of the steps performed under normal, expected conditions to accomplish the goal and expected outcome of the use case. <ol style="list-style-type: none"> 1. Build software
FREQUENCY OF USE:	Daily use, averaging several hours per day.
DATA DESCRIPTION:	Non-sensitive and non-controlled data and files. No different than what would be shared via e-mail or within Microsoft Word. Major difference is improved functionality.

USE CASE:	<i>Collaboratively build open source software</i>
PRIVACY:	Will this use case include any data that has a privacy implication? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Comments: <Describe here>
ADDITIONAL COMMENTS:	The Commerce Data Service will also procure private repositories within the cloud service.

2.4 Appendix D – IT Security Review

Product Name	GitHub	Product Web Site (url)	www.github.com
Name of Assessor	Eric Cline	Email Address	ecline@doc.gov
Date	May 24, 2016		
Recommendation	Approved	<input checked="" type="checkbox"/>	Not Approved <input type="checkbox"/>

Security Assessment

[Describe the methods and tools used for the assessment]

After conducting a simplified review to determine the security controls for GitHub, it is my opinion that this product should be approved for use within the Department of Commerce. See attached security review documentation as evidence to support this determination. It is also recommended that each organization that utilizes GitHub develop additional policies and procedures for its use.

After conducting a simplified review to determine the security controls for GitHub. It is my opinion that this product should be approved for use within the Department of Commerce. The information provided below was utilized as evidence to support this determination. It is also recommended that each organization that utilizes GitHub develop additional policies and procedures for its use.

- A simplified security assessment was completed using NIST SP 800-53 with low baseline controls



GitHub Security Controls Matrix (Low)

- GitHub will not contain Personally Identifiable Information (Use Case)
- GitHub will not contain Business Identifiable Information (Use Case)
- The Department has developed the following guidance for GitHub



Doc_GitHub_Guidance_FINAL.pdf

- GitHub utilizes both organizational and user account permissions



Permission levels for an organization



Permission levels for a user account

- GitHub can employ dual factor authentication
- GitHub is in use by the following Department of Commerce bureaus and has received Authorization to Operate for each Implementation
 - NOAA
 - PTO
 - NIST

- GitHub Security Overview



GitHub Security.pdf

- GitHub Privacy Overview



Privacy github.pdf

- Additional Information provided by NIST



GitHub_Inside NIST.docx



GitHub Frequently Asked Questions.pdf



GitHub_Rules_of_Behavior_2_1.pdf

2.5 Appendix E – Records Management

Background / Depth and Scope

This document assesses GitHub use for the Office of the Chief Data Officer. GitHub is a cloud-based app.

This assessment is constrained by the Use Case defined by the TRB. A reassessment is required if there is a:

- Major change to the app functions to manage records (example: format, ability to export, etc.);
- Major change to the Use Case, including but not limited to the assurance that records are accessible by the Department, and the size of the program’s staff;
- Change of ‘owner’ for this records within the app; and
- Other change which may invalidate the authorization of the system.

This Records Management assessment focusses on conformance with the Federal Records Act, 36 CFR Chapter XII Subchapter B, NARA guidance, and Department policy, as follows:

1. Ensuring a NARA schedule is in place for the authority to dispose of records
2. Ensuring records cleansing and disposition. This includes ensuring both the appropriate authorities are in place, and also procedures for cleansing and disposition. Cleansing and disposition includes the cleaning of non-records, the removal of personal records, the disposal of temporary records in accordance with the authorities granted through the records schedule, or the accessioning of permanent records to the National Archives and Records Administration (NARA)
3. Ensuring the app can produce, manage, and preserve the records in an acceptable electronic format
4. Ensuring the records remain usable and retrievable
5. Ensuring the records are accessible to accommodate agency business, requests for records (such as through litigation discovery or FOIA), and cleansing and disposition. This includes a process to locate records for a records freeze, and export
6. Ensuring the records are findable by the Department. This includes the ability to find the system, such a through a File Plan, an inventory of Department systems, or other means. This also means appropriate search or other functionality to find the record in the system.
7. Ensuring there is a chain of ownership for the records, including a process to ensure succession.

Records and Storage

The scope of the Use Case (Appendix A) includes the following types of records and storage:

- Code segments to build software. These code segments are records of the Department.

- There are no special restrictions such as PII, BII, CUI, or classified materials.
- Users create, access, maintain and store records in the app. The Use Case calls out storage, “*The Commerce Data Service will also procure private repositories within the cloud service.*”

User Base

The user base scope is limited to the Office of the Chief Data Officer, and staff described as “*30+ members of the Commerce Data Service.*” Because GitHub functionality is going to require much of the Records Management functions to be manual, the size of the staff being at a reasonable number approximation of 30 users is doable. Should the number of staff grow significantly above the approximately 30 users, Records Management may be too complex and burdensome to rely on manual execution. In that case, the program should look to tools that provide the automaton of Records Management functions.

Evaluation

This section discusses the evaluation and recommendations.

Line #	Requirement and Reference	Assessment	Recommendation
1	<p>Records are scheduled</p> <p>References/ requiring and communicating the schedule: 36 CFR 1225.10, 36 CFR 1220.18, 36 CFR 1225.12(a)</p> <p>References/ determination of schedules: 36 CFR 1225.10, 36 CFR 1225.12, 44 USC 3303</p> <p>Reference/GRS: 36 CFR 1227</p> <p>Reference/functional analysis for schedules 36 CFR 1225.12</p> <p>Reference/ Records Management staff access: 36 CFR 1225.12</p>	<p>There is no approved records schedule for these records.</p> <p>These records are temporary records. The absence of permanent records has implications in the assessments of other Records Management requirements (below).</p>	<p>Have the program sign a statement that they will work to schedule the records in a reasonable period of time</p>

Line #	Requirement and Reference	Assessment	Recommendation
2	<p>Cleansing and Disposition</p> <p>Reference/ identify and destroy temporary records: 36 CFR 1236.20(b), 36 CFR 1224.10, 36 CFR 1225.18</p> <p>Reference/ culling and removal of non-records: 36 CFR 1222.16, 36 CFR 1225.18(c)</p> <p>Reference/ associate records with disposition authorities: 36 CFR 1236.20, 36 CFR 1225.12, NARA Bulletin 2014-04, 36 CFR 1236.12(b), 36 CFR 1236.20 (b)(6)</p>	<p>GitHub has the appropriate tools to allow a user to self-manage the clearing non-records, the removal of personal records, and the disposal of temporary records.</p> <p>The records are temporary records, resulting in no requirement to accession to NARA.</p>	<p>Make the program aware they are responsible for manually clearing non-records, the removal of personal records, and the disposal of temporary records in accordance with the records schedule.</p> <p>Make the program aware they may not delete any records until a schedule is in place. Until a schedule is in place, they may archive records they wish to delete in a central location, to make the future cleansing easier.</p> <p>Recommend the program write down their processes and procedures in preparation for succession of ownership of the records to the next administration.</p>
3	<p>Acceptable electronic format</p> <p>Reference/ acceptable file formats: 36 CFR 1235.50, NARA Bulletin 2014-04, NARA Bulletin 2013-02</p>	<p>GitHub records can be copied downloaded using a standard browser. However, preserving the metadata will be a manual process for the program.</p>	<p>Make the program aware that they are responsible for maintaining the context and metadata for their records, including the creator, organization, and updates. If the context and metadata needs to be preserved, this may require a manual process and they are responsible for the cost and implementation.</p>
4	<p>Usability, Retrieivability, and Export</p> <p>Reference/ usable and retrievable: 36 CFR 1225.12, 36 CFR 1236.20, 36 CFR 1236.12(b)</p> <p>Reference/ preserve metadata 36 CFR 1236.20</p> <p>Reference/ preserve metadata on creator and organization: 36 CFR 1236.10</p> <p>Reference/ export of metadata: 36 CFR 1235.50, NARA Bulletin 2014-04</p>	<p>GitHub has appropriate tools to allow a user to self-manage the accessibility and retrievability of records.</p> <p>GitHub provides the appropriate context of the creator and organization.</p> <p>If the records need to be migrated, it is up to the user to ensure there is no loss of context or metadata.</p>	<p>Make the program aware that if they migrate data, they must preserve both its context and metadata.</p>

Line #	Requirement and Reference	Assessment	Recommendation
5	<p>Accessibility and ensuring records freezes</p> <p>Reference/ retrievable by other staff as needed: 36 CFR 1225.12, 36 CFR 1236.20</p> <p>Reference/ records freezes: 36 CFR 1236.20(b)</p> <p>Reference/ prevent unauthorized access, modification or deletion: 36 CFR 1236.20</p> <p>Reference/ must be able to access records of current and former employees: 36 CFR 1236.20, 5 U.S.C § 552</p> <p>Reference/ ensure that the records cannot be adulterated or wrongly deleted: 36 CFR 1222.34(d)(2)</p>	<p>GitHub provides the functionality for the program administrator to access the program’s records and control who in their staff has access. This evaluation does not address GitHub’s staff access to the records. The GitHub staff access to records should be addressed by the Cyber-Security assessment.</p> <p>GitHub does not provide appropriate tools to automate a records freeze. However, the program can institute a manual process to accommodate this. The accommodation must ensure an electronic version of the record is saved in the Department’s infrastructure, and done in a way that preserves the context and metadata.</p>	<p>Have the program sign a statement that if there is a records freeze, they will migrate the record to the Department. This will be done in a way that preserves all context and metadata.</p>
6	<p>Findability</p> <p>Reference/ search records of current and former employees: 36 CFR 1236.20, 5 U.S.C. § 552</p> <p>Reference/ search for content and/or attributes: NARA RMS</p>	<p>The program’s instance of GitHub must be included in any current or future inventories of cloud apps, for the purpose of identifying where Department records are located.</p> <p>Within the system, GitHub provides finding aids and code management.</p>	<p>Make the program aware they must comply with all Department initiatives to inventory systems, including those in the cloud.</p>
7	<p>Chain of ownership</p> <p>Reference/ retrievable by other staff as needed: 36 CFR 1225.12, 36 CFR 1236.20</p> <p>Reference/ must be able to access records of current and former employees: 36 CFR 1236.20, 5 U.S.C § 552</p> <p>Reference/ ensure that the records are not wrongly deleted: 36 CFR 1222.34(d)(2)</p>	<p>To ensure the Department always has access to the GitHub records, the program must set up a system to ensure a chain of ownership of the system and access to the records in the system.</p> <p>This process must ensure the records are not wrongly deleted due to abandonment of the cloud account.</p>	<p>Have the program sign a statement that they will ensure succession of ownership of the records. When the organization stops using the app, whether by their choice or the app provider, the organization will ensure all records are migrated into the Department’s infrastructure or a follow on system. This includes records in draft, in use, and in archive.</p>

Recommendations

The recommendation is approval GitHub, with the following:

- In the Use Agreement, signed by the organization using the app, add a statement that the organization accepts responsibility to begin establishment of a records schedule within 90 days of approval, in collaboration with the DOC Chief Records. If the process to create a records schedule is not begun within the 90-day window, the authority to use the app is rescinded.

- In the Use Agreement, signed by the organization using the app, add a statement that the organization accepts responsibility for ensuring records created remain the property of the Department and accessible by the Department.
- In the Use Agreement, signed by the organization using the app, add a statement that the organization will ensure succession of ownership of the records. When the organization stops using the app, whether by their choice or the app provider, the organization will ensure all records are migrated into the Department's infrastructure or a follow on system. This includes records in draft, in use, and in archive.

2.6 Appendix F – Section 508 Compliance

From: Jessup, Jennifer (Federal)
Sent: Thursday, May 26, 2016 3:22 PM
To: Ky, Wes (Federal) <WKy@doc.gov>
Cc: Cavanaugh, Erin (Federal) <ecavanaugh@doc.gov>; Dumas, Sheleen (Federal) <sdumas@doc.gov>; Couch, Wendy (Federal) <WCouch@doc.gov>; Pennington, Thomas (Federal) <TPennington@doc.gov>
Subject: GITHUB Section 508 Recommended Recommendation

As part of the technology review process, I have reviewed the GITHUB technology request in regards to Section 508. My comments are provided below:

The Web Advisory Council (WAC) has previously reviewed and approved GITHUB to be used as a tool to share code and content in the spirit of collaboration and open government. Department of Commerce (DOC) guidance for how DOC uses GitHub is provided at: <https://github.com/CommerceGov/Policies-and-Guidance/blob/master/GithubGuidanceforDepartmentofCommerce.md>.

Section 508 Specifications:

Social Media tools, like other web-based applications, whether inside the DOC network or in the other areas of the Web, must make every **effort to comply with Section 508 and other policies on accessibility, privacy, and record keeping**. In some rare instances, it's not possible to redesign an outside system to be accessible, but it's usually possible to link back to equivalent information on a DOC website. A DOC email address must always be visible on a DOC or DOC bureau GitHub site for users who require alternative methods of accessing the information posted.

To that end, I recommend GITHUB is approved; however, my recommendation is provided **only** if the tool is used in accordance with the Departmental guidance previously approved by the WAC.

Please let me know if you have any questions or need further information from me in regards to this request.

Regards,
Jennifer Jessup
Office of IT Policy and Planning
Office of the Chief Information Officer
Office of the Secretary
United States Department of Commerce
202-482-0336
jjessup@doc.gov

2.7 Appendix G – EA TRM

Product Name	GitHub	Product Web Site (url)	www.github.com
Date	May 31, 2016		
TRM Lead	Tom Pennington	Email	tpennington@doc.gov

Product Evaluation

GitHub will be used as a public source code repository for development work by the Chief Data Officer's office. Currently there are no products in the approved product list with the same or similar capabilities.

Recommendation

Since there are no products already approved that fit the requirements, I recommend that GitHub be approved for use and added to the list of approved products for the Department of Commerce.

X

Thomas J Pennington
Chief Enterprise Architect

2.8 Appendix H – Privacy



UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

June 2, 2016

MEMORANDUM FOR: Steven Cooper
Chief Information Officer

Ian Kalin
Chief Data Officer

FROM: Catrina D. Purvis **Catrina D. Purvis**
Senior Agency Official for Privacy (SAOP) &
Chief Privacy Officer

SUBJECT: Privacy Impact Assessment (PIA) Requirement for
Departmental Use of GitHub and Similar Freeware Tools

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary,
ou=Office of Privacy and Open Government, ou=US
Department of Commerce, email=cpurvis@dot.gov,
c=US
2016.06.02 12:57:48 -0400

This memorandum responds to the inquiry received on May 26, 2016, from the Office of the Chief Information Officer (OCIO) about whether a new SAOP approved privacy impact assessment (PIA) is required, prior to approval/ authorization of GitHub (and other similar freeware tools) for Departmental uses which will include personally identifiable information (PII) and other Privacy Act protected information.

GitHub specifically, is a third-party website which offers code repositories that developers can use to collaborate on software development projects. As such, GitHub may be considered a social networking platform which may be covered by the existing SAOP approved Departmental PIA entitled, “Third Party Social Media Websites and Applications” (see attached). Please instruct your teams to review the aforementioned PIA to advise you on whether it is applicable to and covers the intended use(s) of GitHub and/ or similar freeware tools for which approval/ authorization is sought.

If the existing PIA is applicable and the intended use(s) are covered, then no new or separate SAOP approved PIA is required. However if not, then a new SAOP approved PIA will be required prior to any collection, storage, processing and/ or dissemination of PII or Privacy Act protected information within GetHub or any similar freeware tool. The new PIA must include the following and template is available:

- the purpose of using GitHub and/or the similar freeware tool;
- terms of service;
- the type of personally identifiable information (PII) and/or Business Identifiable Information (BII);
- intended or expected use of PII/BII;
- the sharing or disclosure of PII/BII;
- the maintenance and retention of PII/BII;
- the protection of PII/BII; and
- the identification and mitigation of other privacy risks, creation or modification of a system of records, and notice and consent.

Pursuant to the Privacy Act of 1974 and Department privacy policy, neither GitHub nor any similar freeware tool can be used in the Department to collect, maintain, or disseminate PII/BII, unless an SAOP approved PIA which covers its intended use(s) is published. Additionally, if PII is collected and maintained in a Privacy Act system of records, which means information is retrieved by the name of the individual or by some other identifying particular assigned to the individual, then according to the Privacy Act, a proper System of Records Notice (SORN), must be published in the *Federal Register*.

Please let me know if you require any additional information or clarification regarding this matter. Ms. Lisa Martin and Mr. Michael Toland are my POCs for this matter and can be reached at LMartin1@doc.gov and MToland@doc.gov, respectively.

Attachment: Third Party Social Media Websites and Applications PIA