



Open Source in the Federal Government

Whoami – Solomon Rubin

- **Software & Security Engineer**
- Long Time Federally Funded Research and Development Center Employee
 - MITRE
 - MIT Lincoln Laboratory
- Work in the Government Open Source Arena
 - Cyber Defense
 - Military
 - Aerospace

On the Web

- @serubin_
- <https://serub.in>

Overview

- How the Government uses code
- How Open Source fits into USG
- Where Open Source occurs
- What Open Source Process looks like
- How it can be improved



How the Government Uses Code

- Code is everywhere
- Technology is ubiquitous in all industries
 - Government is no exception
- All industries are ultimately technology industries first



What kind of code does the Government use?

- Data science
- Cyber security and digital forensics
- Full stack & web engineering
- Much more

What kind of code does the Government use?

- **Data science**
- Cyber security and digital forensics
- Full stack & web engineering
- Much more



What kind of code does the Government use?

- Data science
- **Cyber security and digital forensics**
- Full stack & web engineering
- Much more



What kind of code does the Government use?

- Data science
- Cyber security and digital forensics
- **Full stack & web engineering**
- Much more



The .gov means it's official.

Federal government websites often end in .gov or .mil. Before sharing sensitive information, make sure you're on a federal government site.



The site is secure.

The **https://** ensures that you are connecting to the official website and that any information you provide is encrypted and transmitted securely.



e-QIP

Login

Identify Yourself to the e-QIP System

Help

The United States Government U.S. Office of Personnel Management (OPM)

Only persons specifically authorized to do so may access this data. Unauthorized attempts to pass this screen, as well as any use of data in this system for purposes other than those authorized by OPM, are a violation of federal law and/or regulation. Violators are subject to disciplinary action and prosecution.

This application is designed to collect sensitive but unclassified data which will be maintained and protected as such by the United States Government. Users must not enter Classified information into this system.

This U. S. government system is to be used by authorized users only. Information from this

What kind of code does the Government use?

- Data science
- Cyber security and digital forensics
- Full stack & web engineering
- **Much more**



The Government is Invested in Open Source

High Engagement - With Large Challenges

- Politically charged environment
- External actors push against OS
- Internal actors push against OS
- Extreme sensitivities exist within the work





External Actors Push against Open Source?

Claimed

- USG **should not** emulate fast paced innovation of Silicon Valley.
- In-house government IT is **not necessary**

- In 2017 an Oracle Executive (SVP) commented on a GSA modernization repo with a scathing review of OS

Suggested

- Security in Open Source is not good enough for government
- Code maintained by a community is not safe
- In conclusion, buy Oracle software



Internal Actors?

Using

- Distrust in “unknown” communities
- Internal code verification
- Negative opinions from agencies

Contributing

- Internal sensitivities make developing OS extremely hard
- Sensitive Information
- Intense code review and legal process



Story - OSCON 2016

NSA Cryptologist



Where in US Government is Open Source Occurring?

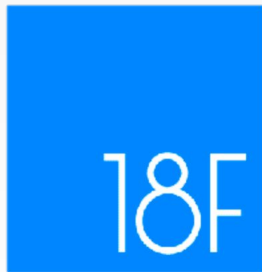
A Changing Environment

- **5 years ago** – policies and the environment **did not** allow for easy open source usage or contribution
- **Today** – Several Open Source “centers” exist with USG
- All Agencies and Organizations use Open Source in some way





Where are the Open Source centers in USG?








What about agencies?

- Agency for International Development
- Consumer Financial Protection Bureau
- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Education
- **Department of Energy (1600)**
- Department of Health and Human Services
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of Justice
- Department of Labor
- Department of the Treasury
- Department of Transportation
- Department of Veterans Affairs
- Environmental Protection Agency
- Executive Office of the President
- Federal Election Commission
- **General Services Administration (2000)**
- **National Aeronautics and Space Administration (1200)**
- National Archives and Records Administration
- National Science Foundation
- National Security Agency
- Office of Personnel Management
- Small Business Administration
- Social Security Administration



Code.Gov

- USG's platform for sharing America's open source software
- Provides a list of existing projects
- Provides Agency Compliance
 - Consistency with the Federal Source Code Policy.
 - Amount of custom software open sourced (~20%)
 - Amount of custom software inventoried (~50%)

	Department of Defense Non-compliant <ul style="list-style-type: none">Agency policy has not been reviewed for consistency with the Federal Source Code Policy.Agency has open sourced less than 10% of their custom developed code.Agency has inventoried less than 50% of new custom code.
	Department of Education Partially compliant <ul style="list-style-type: none">Agency policy is consistent with the Federal Source Code Policy.Agency has open sourced greater than 20% of their custom developed code.Agency has inventoried less than 50% of new custom code.
	Department of Energy Fully compliant <ul style="list-style-type: none">Agency policy is consistent with the Federal Source Code Policy.Agency has open sourced greater than 20% of their custom developed code.Agency has inventoried 100% of new custom code.

code.gov

What does USG Open Source Look Like?

- Open Source – USG's Contributions

- Common Vulnerabilities and Exposures
- STIX & TAXII
- Ghidra
- SHA
- Simon/Speck
- Code.gov

- Inner Source – USG Works Together

- Licenses for government wide reuse
- Reuse within agencies is common
- Inter-agency code sharing is frequently



What makes USG's Needs different?

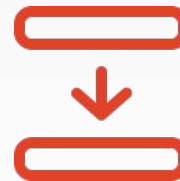
Special Sensitivities



**Rigorous Hosting
Regulation**



**Precautions for
Classifications**





Government Process

Library Level Approval



Rigorous External Release Process



Classified Process

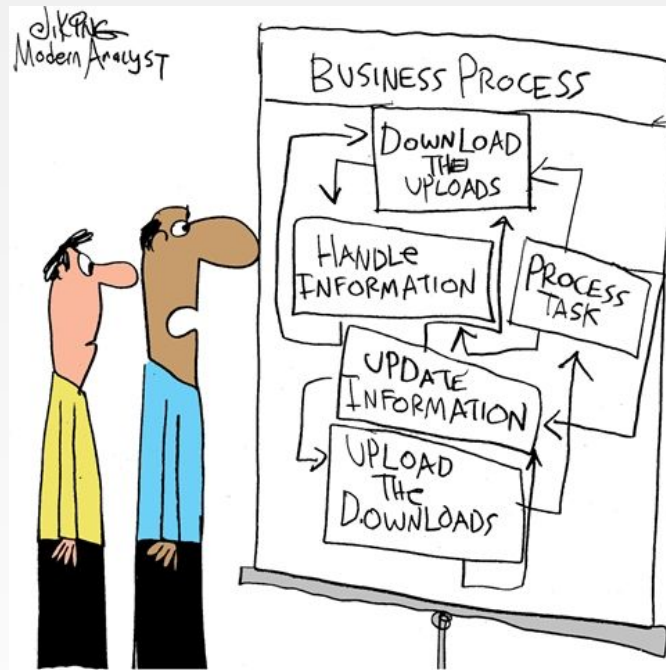
- Heavily scrutinized
- Largely Done Unclassified
- Requires an extra level of security analysis





How can this improve?

- **Better process!**
- Automate manual reviews
- Pre-approve common libraries
- Better policy



“Charlie, did you really get these details from the customer?”



Commitment to Open Source

- Educate on **value**
- Educate on **availability**
- Educate on **safety**
- Support USG open source initiatives





serub.in/gitlab-commit-2019

Slides and Additional Information