# Transparent code, secure data

*Selling Free Software to the US Government, our Bosses, and Ourselves*

Fen Labalme and Karen Johnson, CivicActions

# Introductions

*Who are we?  What do we do?  Why should you care?*

# Who We Are:

Fen Labalme: CISO, CivicActions

Karen Johnson: DevSecOps Engineer, CivicActions

http://www.durfee.net/startrek/DS9_0216.html

# Why do we care about this?

# And why should you?

https://imgflip.com/i/1z4bu1

## Why do we care about this?

➔ *We're nerds.*

## And why should you?

➔ *Because the US government should use tax dollars to make ethical choices and serve the people.*

https://imgflip.com/i/1z4bu1

# Why isn’t the whole world using free software?

*Common concerns, misconceptions, and some valid criticisms of free software*

# Why not free software?

1. Free Software doesn’t work for my needs!
2. Free Software is insecure!
3. Free Software is buggy!
4. Change is hard!

# It Doesn’t Work!

- ➔ Free software options are less intuitive, or have less emphasis on UX
- ➔ It works differently
- ➔ README files are too technical
- ➔ May be designed for GNU/Linux

https://www.pinterest.com/pin/343469909059554706/?lp=true

## Readable README files

- Documentation is not QA'd by non-technical users
- We may be to blame, too. Be proactive and create simple readability pull requests

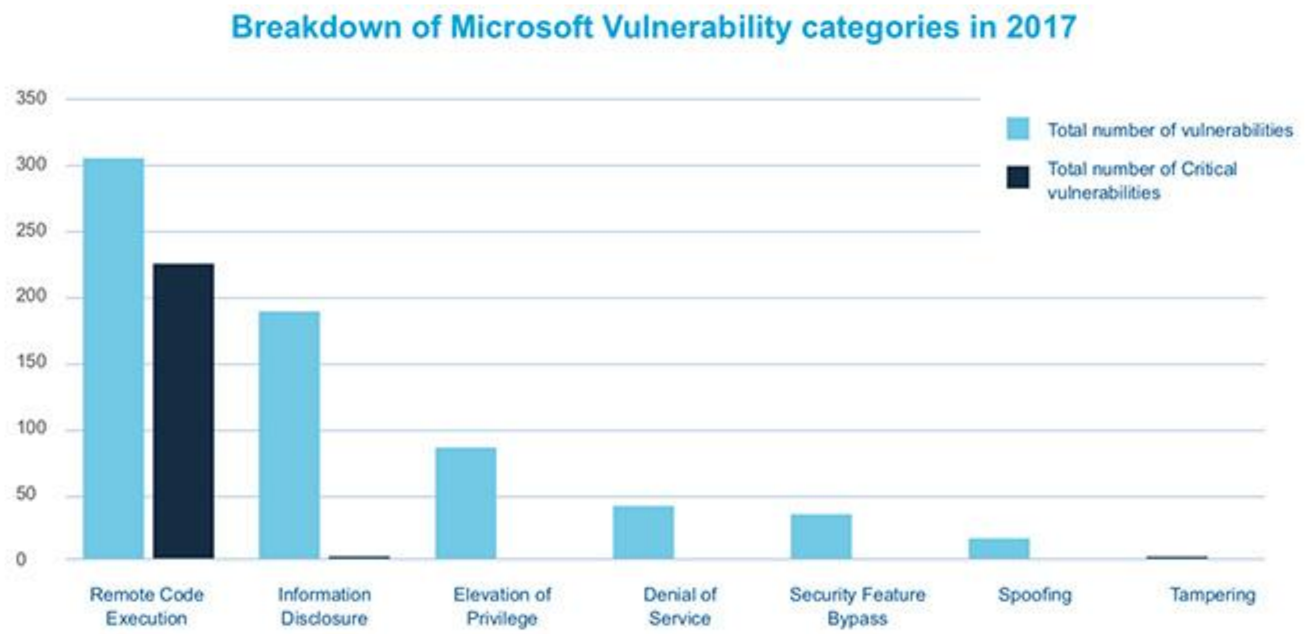
## GNU/Linux is the way

- While we'd like everyone to use GNU/Linux, Windows is still prevalent
- Consider releasing setup instructions for Windows users

## Why not free software?

1. Free Software doesn’t work for my needs!
2. **Free Software is insecure!**
3. Free Software is buggy!
4. Change is hard!

# Why not free software?



https://www.helpnetsecurity.com/2018/02/15/reported-windows-vulnerabilities/

# It’s insecure!

- ➔ If it’s open for scrutiny, then anyone can go through the source code and discover potential exploits.
- ➔ Keeping a security or encryption algorithm proprietary is the only way to ensure it not being cracked.
- ➔ Since it’s free software, nobody cares about maintaining it or applying security updates
- ➔ Micro$oft is a big company and they sell to the government, so they must be secure

# Encryption must be proprietary? No!

- **Bruce Schneier**: “demand OSS for anything related to security”
- **Vincent Rijmen**: “forces people to write more clear code & adhere to standards”
- **Whitfield Diffie**: “it’s simply unrealistic to depend on secrecy for security”
- **Jerome Saltzer (1975):** “Open design: The mechanisms should not depend on the ignorance of potential attackers” http://web.mit.edu/Saltzer/www/publications/protection/index.html

## Why not free software?

1. Free Software doesn’t work for my needs!
2. Free Software is insecure!
3. **Free Software is buggy!**
4. Change is hard!

# It’s buggy!

Years ago we used to have debates about whether open source or proprietary software was higher quality, by which we mostly meant fewer bugs. Coverity's reports each year showed that, in fact, free and open-source software did have a lower bug density on average. https://www.synopsys.com/blogs/software-security/2017-coverity-scan-report-open-source-security/

**4,600**

Active Free Software projects

**600,000**

Fixed defects (from 2008 to 2017 report)

# It’s buggy? Not as buggy as proprietary...

*“The internal structure of proprietary software is strictly closed-access meaning they lack transparency which makes it virtually impossible for users to even suggest modifications or optimizations to the software. Open source, on the other hand, promotes open collaboration which means lesser bugs and faster bug fixes with fewer complexities.”*
[http://www.differencebetween.net/technology/difference-between-open-source-and-proprietary-software/](http://www.differencebetween.net/technology/difference-between-open-source-and-proprietary-software/)
(2020)

[https://www.syfy.com/syfywire/william-shatner-on-whether-hell-appear-on-star-trek-discovery](https://www.syfy.com/syfywire/william-shatner-on-whether-hell-appear-on-star-trek-discovery)

# Why not free software?

1. Free Software doesn’t work for my needs!
2. Free Software is insecure!
3. Free Software is buggy!
4. **Change is hard!**

# Change is hard!

Why would I switch to using some other software, when the thing I currently use already works for me?

Additionally, why should a company pay for infrastructure changes to use free software?

https://imgur.com/C9QFLRy

# Case Studies from our own organization:

*Free Software Beliefs at CivicActions*

# What We’ve Done:

*Championed the use of free software over proprietary solutions:*

- ➔ **Drupal over proprietary CMS choices**
  - All of our projects!
- ➔ **GNU/Linux over Windows**
- ➔ **Moodle over Blackboard**
  - DAEL (Dept. of Adult Literacy)
- ➔ **OpenSCAP and ZAP for scanning over Tenable Nessus**
  - Building a compliance automation stack using free software
- ➔ **Mattermost over Slack**
  - DoD Peacekeeping Wing

# What We’ve Done:

*Feedback on the Defense Digital Services’ https://code.mil licensing strategy*

*We’ve provided training for government lawyers and procurement officers on using FOSS*

*Our leadership sits on the board of the Free Software Foundation*

- ➔ *Henry Poole:* https://www.fsf.org/about/staff-and-board

https://www.fsf.org/resources/badges

# What We’ve Done:

## *What hasn’t worked so well?*

- ➔ *We’ve lost contracts because they wouldn’t go with a free software solution.*
- ➔ *We’ve run into requirements to use proprietary security tools, which mean we can’t implement our own free software solutions.*

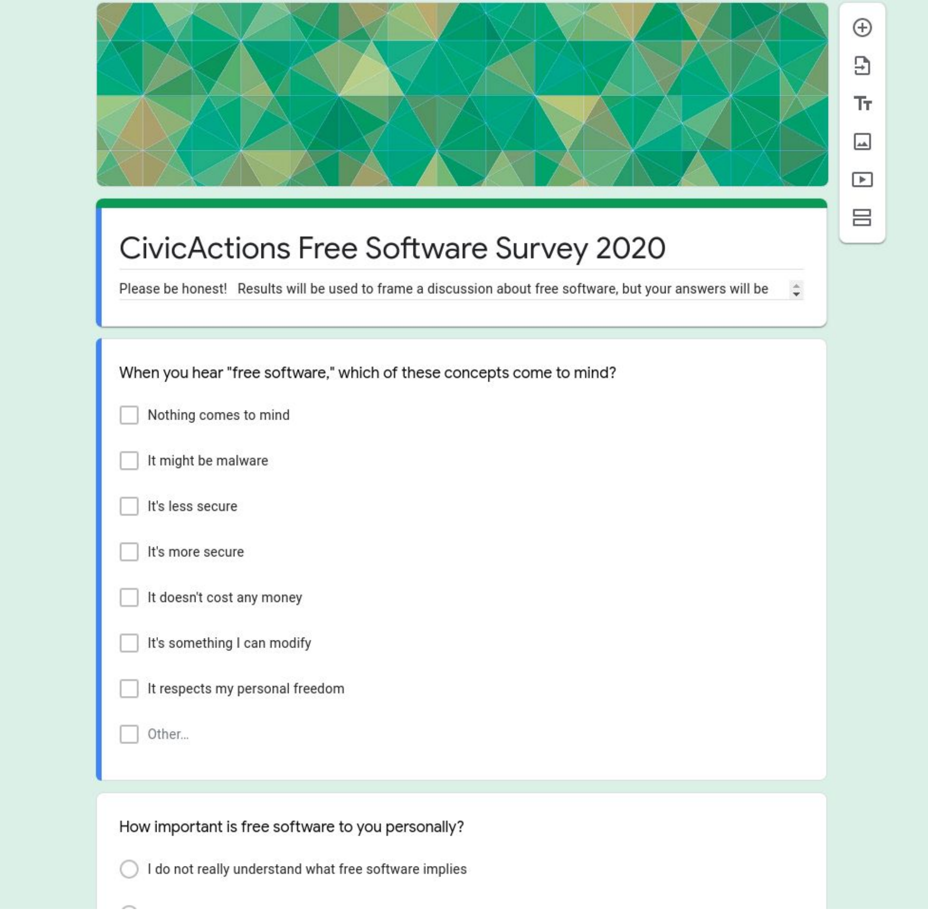
https://en.wikipedia.org/wiki/File:Redshirt_characters_from_Star_Trek.jpg

# Takeaways from Client Work:

- ➔ *We can still have impact, even when a contract already knows and wants a free software tool.*
- ➔ *Word of mouth is really important.*
- ➔ *We should focus our efforts on figuring out how to change perceptions of free software, so that it doesn't automatically prohibit us from taking on work that has used a proprietary solution in the past.*

# What We've Done: *Internal Initiatives*

*Surveyed our own coworkers to assess their education level around free software*



CivicActions Free Software Survey 2020

Please be honest! Results will be used to frame a discussion about free software, but your answers will be

When you hear "free software," which of these concepts come to mind?

- □ Nothing comes to mind
- □ It might be malware
- □ It's less secure
- □ It's more secure
- □ It doesn't cost any money
- □ It's something I can modify
- □ It respects my personal freedom
- □ Other...

How important is free software to you personally?

- ○ I do not really understand what free software implies

# Our Free Software Survey Questions:

*When you hear “free software,” which of these concepts come to mind?*

*How important is free software to you personally?*

*How important do you feel free software is/should be to CivicActions?*

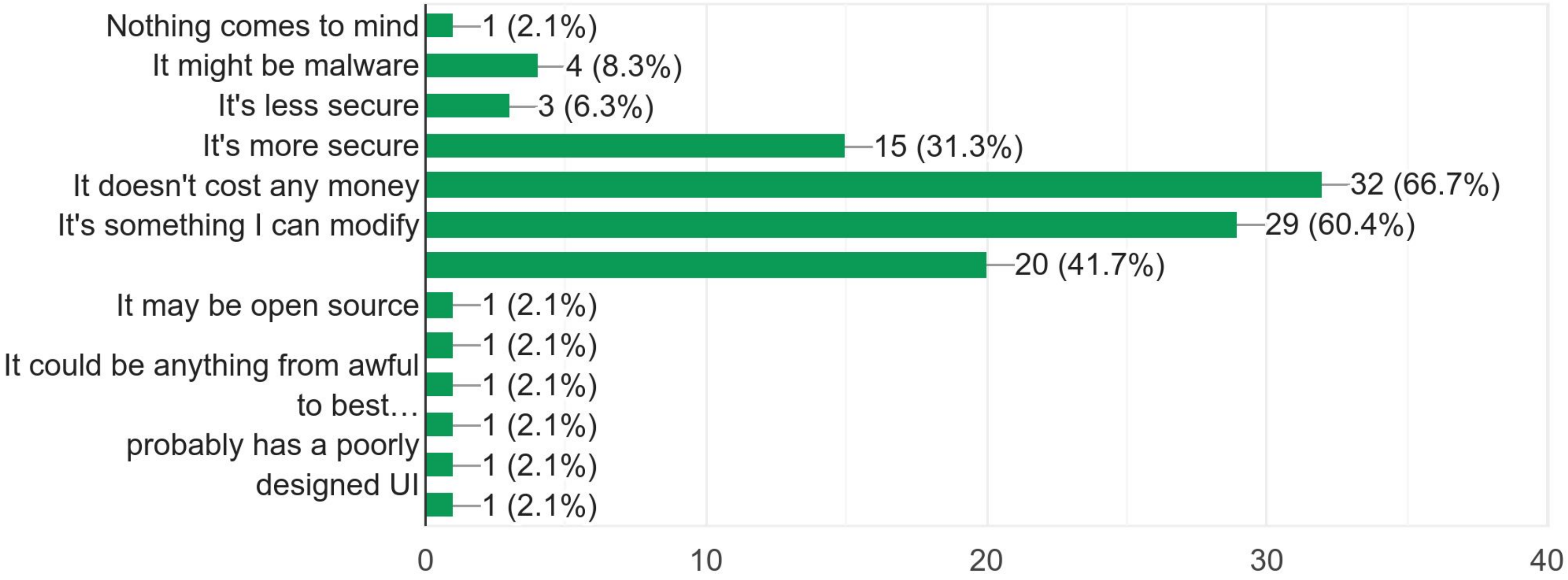
*Should CivicActions emphasize the use of free software in new contracts?*

*Should CivicActions emphasize the use of free software for internal company use?*

# Case Studies

When you hear "free software," which of these concepts come to mind?

48 responses



# Responses:

**8.3%**
It might be malware

**6.3%**
It's less secure

**31.3%**
It's more secure

**66.7%**
It doesn't cost money

**60.4%**
It's something I can modify

# Responses:

“It respects my personal freedom.”

“It might be a for-profit scheme which might involve ads and tracking data.”

“It probably has a poorly designed UI”

“It might not be very good software and might not be adequately supported.”

“It could be anything from awful to best of breed.”

# What we learned:

- ➔ **Even though our business is based on ethical work and utilizing free software, there are lots of misconceptions inside our own workplace.**

- ➔ **Opinions about free software are diverse and varied across our company.**

# So what can we do?

*Ideas for championing free software in your organization*

1. **Reframe how we talk about change**
2. Educate the people!
3. Counter Misinformation
4. Do your part to make free software user friendly
5. Be part of the conversation about new solutions

# Upgrade mentality vs. “changing what works”:

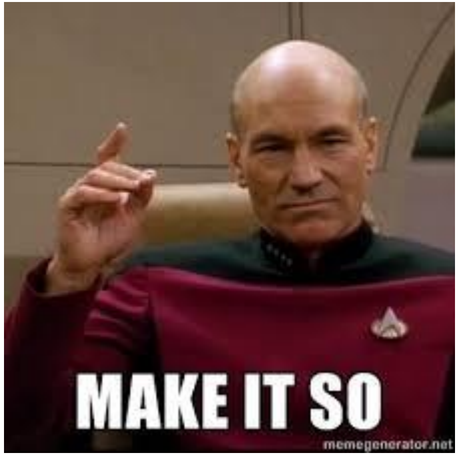
- ➔ Frame a move to free software as an “upgrade,” rather than a change away from something that already works. In tech fields, we are constantly upgrading to newer and better solutions, so use this language to talk about shifting to free software solutions over proprietary ones.

## Be a free software champion!

1. Reframe how we talk about change
2. **Educate the people!**
3. Counter Misinformation
4. Do your part to make free software user friendly
5. Be part of the conversation about new solutions

# Education:

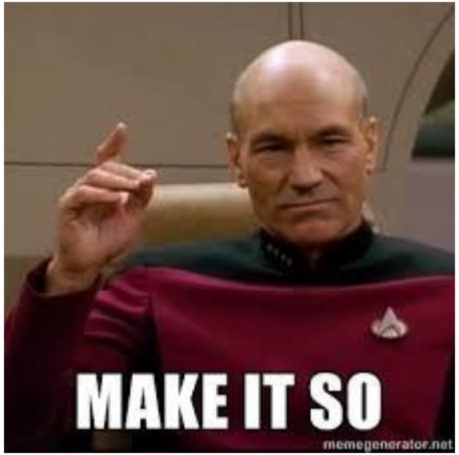
- ➔ First, educate yourself. What products do you really like? What concerns have you heard from your friends, family, and coworkers, and can you give them an honest and accurate answer? Consider a quiz to find out where your team is at with free software knowledge and awareness.



https://www.pinterest.com/pin/90072061269841695/?lp=true

# Education:

- ➔ Be aware of free software in the wild!
- ➔ Is your organization already using free software that you like? Make sure people know that!



https://www.pinterest.com/pin/90072061269841695/?lp=true

# Education:

*What does free software mean to you?*

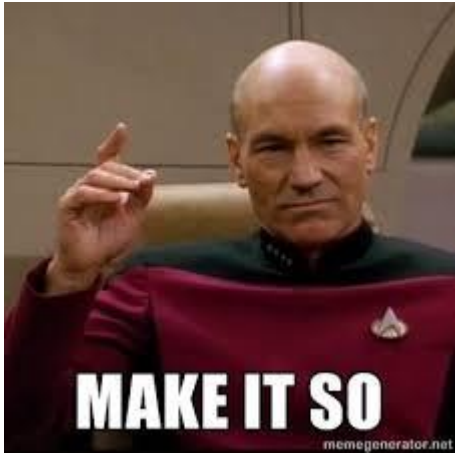
**Freedom to create:** GIMP, Blender, Gifsicle, ImageMagick, Inkscape

**Freedom to learn:** moodle, ATLAS, GnuSchool, KidsRuby, Moodle, OpenGrade,

**Freedom to manage your productivity:** RecordMyDesktop, Recruit, LibreOffice, HomeBank, Ledger

**Freedom to protect your privacy:** IceCat, Tor, OpenVPN, GPG, NoScript, HTTPS Everywhere, Ricochet, Electrum, SecureDrop

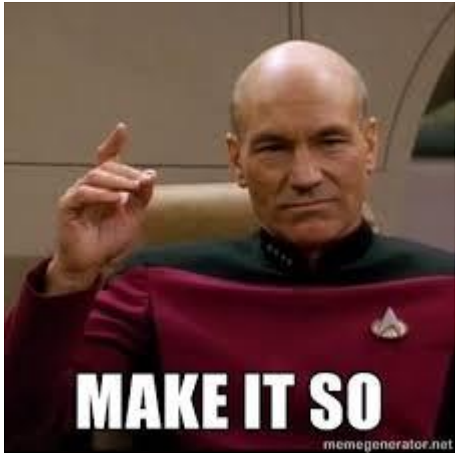
More tools at: https://directory.fsf.org/wiki/Main_Page



https://www.pinterest.com/pin/90072061269841695/?lp=true

# Education:

➔ Consider utilizing your company’s social resources to educate people about the benefits of free software.



https://www.pinterest.com/pin/90072061269841695/?lp=true

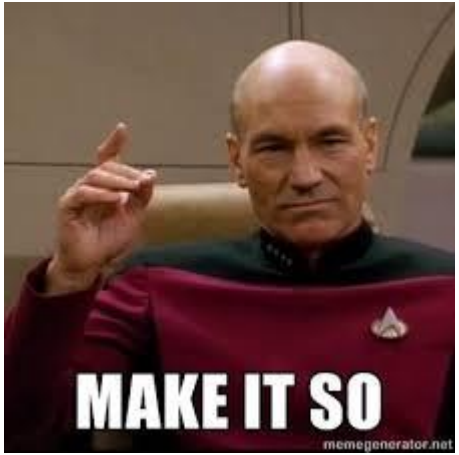
# Education:

*What's in a name?*

➔ Help people understand what "free software" actually means.

➔ Free as in beer -> Freedom respecting

***"Free software is software that respects your freedom."***



https://www.pinterest.com/pin/90072061269841695/?lp=true

## Be a free software champion!

1. Reframe how we talk about change
2. Educate the people!
3. **Counter Misinformation**
4. Do your part to make free software user friendly
5. Be part of the conversation about new solutions

# Counter Misinformation:

- 8 of the 10 Most Exploited Bugs Last Year Involved Microsoft Products
  https://www.darkreading.com/vulnerabilities---threats/8-of-the-10-most-exploited-bugs-last-year-involved-microsoft-products/d/d-id/1336968
- The DoD's OSS FAQ states that "*continuous and broad peer-review, enabled by publicly available source code, improves software reliability and security through the identification and elimination of defects that might otherwise go unrecognized.*"
  https://dodcio.defense.gov/Open-Source-Software-FAQ/

# Defense Innovation Board

From the DoD Software Acquisition and Practices (SWAP) Study: “*DoD should use open source software when possible to speed development and deployment and leverage the work of others.*”

https://innovation.defense.gov/software/

# Digital Services Playbook

- ➔ Encourages agencies to “*default to open*”
- ➔ “software and data generated by third parties remains under [the U.S. Government’s] control, and can be reused and released to the public as appropriate and in accordance with the law.”
- ➔ “helps government build effective digital services.”
  [https://playbook.cio.gov/](https://playbook.cio.gov/)

# Federal Source Code Policy

“requires agencies, when commissioning new custom software, to release at least 20 percent of new custom-developed code as Open Source Software (OSS)”

https://sourcecode.cio.gov/

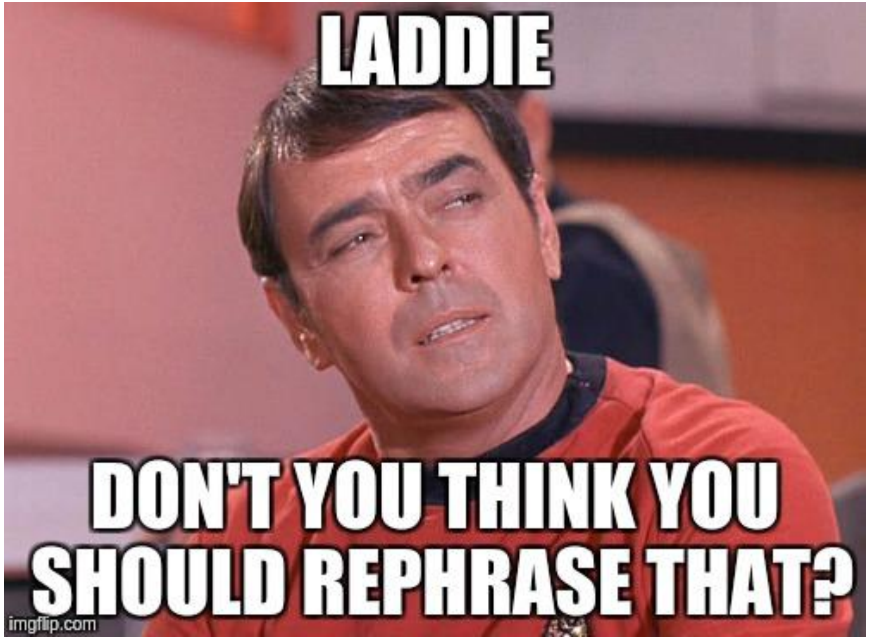
# Federal Source Code Policy in use

- **Social Security Administration** (SSA)  (initially 10/3/2016)
  https://www.ssa.gov/digitalstrategy/m_16_21_Implementation_Plan.html
- **GSA** Open Source Software Policy (initially 11/3/2016)
  https://www.gsa.gov/directives-library/gsa-open-source-software-oss-policy-21071-cio
- **NASA** Federal Source Code Framework (11/15/2016)
  https://code.nasa.gov/NASA-M-16-21-Framework.pdf
- **EPA**: Interim Open Source Software (OSS) Policy (1/11/2018)
  https://www.epa.gov/open/interim-open-source-software-oss-policy
- https://code.gov/ - “Sharing America’s Code”

1. Reframe how we talk about change
2. Educate the people!
3. Counter Misinformation
4. **Do your part to make free software user friendly**
5. Be part of the conversation about new solutions

# Do your part:

1. QA your documentation. Have others read it for clarity and ease of use.
2. When working with users, work to include and empower, rather than condescend.
3. Consider options to make your project easier to trust and incorporate.



https://imgflip.com/i/20fzw6

# The Linux Foundation

Core Infrastructure Initiative (CII)

**Best Practices Badge Program**

https://bestpractices.coreinfrastructure.org

kubernetes
HYPERLEDGER
node
JS
LibreOffice
curl://
GitLab
Prometheus
pkgsrc
Xen Project
openstack
NVM
Zephyr
Syncope
libcloud
OpenSSL
BRLCAD
Nextcloud
GnuPG
GNU Make
blender
OPNFV

# Best Practices Badge Criteria include

- *FLOSS License*
- *Basic project website content and documentation*
- *Public version-controlled source repository*
- *Unique version numbering and release notes*
- *Bug and vulnerability reporting process*
- *Automated test suite*

# A few best practices from a security guy

Use basic good cryptographic practices - e.g., don’t roll your own, use well-known and vetted free libraries, viz libsodium.org & keycloak.org

https://security.stackexchange.com/questions/18197/why-shouldnt-we-roll-our-own (answers from 2012 -> 2019)

OWASP - The Open Web Application Security Project

- ➔ https://owasp.org/www-project-top-ten/
- ➔ https://owasp.org/www-project-api-security/

Automated test suite: Hosted GitLab runner available for free

## Be a free software champion!

1. Reframe how we talk about change
2. Educate the people!
3. Counter Misinformation
4. Do your part to make free software user friendly
5. **Be part of the conversation about new solutions**

# Be Part of the Conversation:

- When a team needs a new tool, make sure a free software tool is one of the options and explain its benefits

https://1.bp.blogspot.com/-MidFu1gVwRI/WtSdjA22dTI/AAAAAAAAU7o/wcx7Vphwx2YjJiFrxnTFB7EOsFf4FPGWACLcBGAs/s1600/star-trek-original-series-uhura-miniskirt.jpg

# Thank You.

- Fen Labalme <fen.labalme@civicactions.com>
- Karen Johnson <karen.johnson@civicactions.com>

https://github.com/CivicActions

*We're hiring!*

# Questions?<br>Suggestions?<br>Success stories?

# Links and References

Slide 3: Odo and Dax image from Deep Space 9: http://www.durfee.net/startrek/DS9_0216.htm

Slide 4-5: Image of Spock saying “fascinating:” https://imgflip.com/i/1z4bu1

Slide 8: Printer with sign depicting McCoy saying, “It’s dead, Jim: https://www.pinterest.com/pin/343469909059554706/?lp=true

Slide 11: Graph of Microsoft Vulnerabilities, 2017: https://www.helpnetsecurity.com/2018/02/15/reported-windows-vulnerabilities/

Slide 15: Quote Attribution: https://www.synopsys.com/blogs/software-security/2017-coverity-scan-report-open-source-security/

Slide 16: Image of Kirk with Tribbles: https://www.syfy.com/syfywire/william-shatner-on-whether-hell-appear-on-star-trek-discovery
Quote attribution: http://www.differencebetween.net/technology/difference-between-open-source-and-proprietary-software/

Slide 18: Image of TOS and new movie Star Trek characters: https://imgur.com/C9QFLRy

Slide 21: Fan of FSF image:https://www.fsf.org/resources/badges, Links from slide: https://code.mil and https://www.fsf.org/about/staff-and-board

Slide 22: Image of Star Trek redshirts: https://en.wikipedia.org/wiki/File:Redshirt_characters_from_Star_Trek.jpg

Slide 24, 26: Screencap of CivicActions survey (taken by us)

Slide 34-38: Image of Captain Picard saying “Make it So:” https://www.pinterest.com/pin/90072061269841695/?lp=true , also link on slide 35: https://directory.fsf.org/wiki/Main_Page

# Links and References

Slide 40: Links from slide: https://www.darkreading.com/vulnerabilities---threats/8-of-the-10-most-exploited-bugs-last-year-involved-microsoft-products/d/d-id/1336968 , https://dodcio.defense.gov/Open-Source-Software-FAQ/

Slide 41: Link from slide: https://sourcecode.cio.gov/

Slide 42: https://www.ssa.gov/digitalstrategy/m_16_21_Implementation_Plan.html , https://www.gsa.gov/directives-library/gsa-open-source-software-oss-policy-21071-cio , https://code.nasa.gov/NASA-M-16-21-Framework.pdf, https://www.epa.gov/open/interim-open-source-software-oss-policy

Slide 43: Link from slide: https://innovation.defense.gov/software/

Slide 44: Link from slide: https://playbook.cio.gov/

Slide 46: Image of Scotty saying ,"Laddie, don't you think you should rephrase that?" https://imgflip.com/i/20fzw6

Slide 47: Graphic of CII badgeholders: https://bestpractices.coreinfrastructure.org/en

Slide 49: Links from slide: libsodium.org & keycloak.org, https://security.stackexchange.com/questions/18197/why-shouldnt-we-roll-our-own , https://owasp.org/www-project-top-ten/, https://owasp.org/www-project-api-security/

Slide 51: Image of the TOS crew: https://1.bp.blogspot.com/-MidFu1gVwRI/WtSdjA22dTI/AAAAAAAAU7o/wcx7Vphwx2YjJiFrxnTFB7EOsFf4FPGWACLcBGAs/s1600/star-trek-original-series-uhura-miniskirt.jpg