



MIS|TI™ PRESENTS

**InfoSecWorld**  
Conference & Expo 2018

# **ANALYZING YOUR GOVERNMENT CONTRACT CYBERSECURITY COMPLIANCE**

*Robert E. Jones*

*Government Contracts & Accounting Expert*

# POSITIVE SHARE



# SAFETY CHECK





# POLL

How many work in or with government contractors?

How many are familiar with Federal Acquisition Regulations (FAR)?

Defense Federal Acquisition Regulation Supplement (DFARS)?

# A LITTLE HISTORY

Health Information Portability and Accountability Act of 1996 (HIPAA)  
HIPAA Privacy Rule & HIPAA Security Rule

Gramm-Leach-Bliley Act of 1999  
Financial institutions

Federal Information Security Management Act (FISMA) of 2002

Federal Information Security Modernization Act (FISMA) of 2014

Federal Information Technology Acquisition Reform Act (FITARA) of 2014

# FAR RULE

## Federal Acquisition Regulation

### FAR 52.204-21

Focus on systems, not data

15 requirements that “most prudent businesses follow.”

Applicable to most federal acquisitions

The screenshot shows a web browser window with the URL [https://www.acquisition.gov/far/html/52\\_200\\_206.html](https://www.acquisition.gov/far/html/52_200_206.html). The browser's address bar and tabs are visible at the top. The main content area displays the text of FAR 52.204-21, titled "52.204-21 Basic Safeguarding of Covered Contractor Information Systems." The text is as prescribed in 4.1903, inserting the following clause:

BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

(a) Definitions. As used in this clause—

- “Covered contractor information system” means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.
- “Federal contract information” means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.
- “Information” means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).
- “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information ([44 U.S.C. 3502](#)).
- “Safeguarding” means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

- (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.
- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.
- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

**52.204-22 Alternative Line Item Proposal.**

As prescribed in [4.1008](#), insert the following provision:

ALTERNATIVE LINE ITEM PROPOSAL (JAN 2017)



# DFARS RULE

## Defense Federal Acquisition Regulation Supplement

### DFARS 252.204-7012

Focus on data, not systems

Requires compliance with NIST 800-171

Applicable to most DoD acquisitions

Dozens of people working on s... X dfars 252.204-7012 - Google S... X 252.204-7000 Disclosure of Informa... X +

Under Secretary of Defense for ... (US) | https://www.acq.osd.mil/dpap/dars/dfars/h

252.204-7012 **Safeguarding Covered Defense Information and Cyber Incident Reporting.**  
As prescribed in 204.7304(c), use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016)

(a) *Definitions.* As used in this clause—

“Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Contractor attributional/proprietary information” means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered contractor information system” means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

“Covered defense information” means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

- (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
- (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

“Operationally critical support” means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

“Rapidly report” means within 72 hours of discovery of any cyber incident.

[www.archives.gov/cui/registry/category-list.html](http://www.archives.gov/cui/registry/category-list.html)

# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Controlled Unclassified Information (CUI) is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.



# CUI REGISTRY

24 categories and 92 subcategories


Includes data generated by the government and by contractors

Dozens of people working on s

CUI Registry - Categories and S

https://www.archives.gov/cui/registry/category-list

Daily Clients Left Brain Resources Personal Professional Web Tools Work Photography Pride Yum


NATIONAL ARCHIVES

[Blogs](#) · [Bookmark/Share](#) · [Contact Us](#)

RESEARCH OUR RECORDSVETERANS' SERVICE RECORDSEDUCATOR RESOURCESVISIT USAMERICA'S FOUNDING DOCUMENTS

Controlled Unclassified Information (CUI)

Home > Controlled Unclassified Information (CUI) > Registry - Categories and Subcategories > CUI Registry - Categories and Subcategories



CONTROLLED UNCLASSIFIED INFORMATION

[Use the CUI logo](#)  
[Contact Us](#)

About CUI

- Key Elements of CUI
- Chronology and History
- FAQs

CUI Registry

- Categories-Subcategories
- Category-Subcategory Markings
- Limited Dissemination Controls
- Decontrol
- Registry Change Log
- Policy and Guidance
- Glossary

CUI Reports

CUI Training Tools

CUI Additional Tools

CUI Registry – Categories and Subcategories

\*\*\*\*\* IMPLEMENTATION REMINDER FROM THE EXECUTIVE AGENT \*\*\*\*\*

Existing agency policy for all sensitive unclassified information remains in effect until your agency implements the CUI program. Direct any questions to your agency's CUI program office.

Search the Registry

CUI Categories and Subcategories

- Select a Category or Subcategory to view associated detail information.
- Unless noted, CUI may be controlled at the Category or the Subcategory level.

Category	Category Description
POSSESSORS OF INFORMATION RELATING TO THE NATIONAL DEFENSE	

# MARKING CUI

CUI supposed to be marked

Media containing CUI  
supposed to be marked

This may be the number one  
failure point for many  
contractors

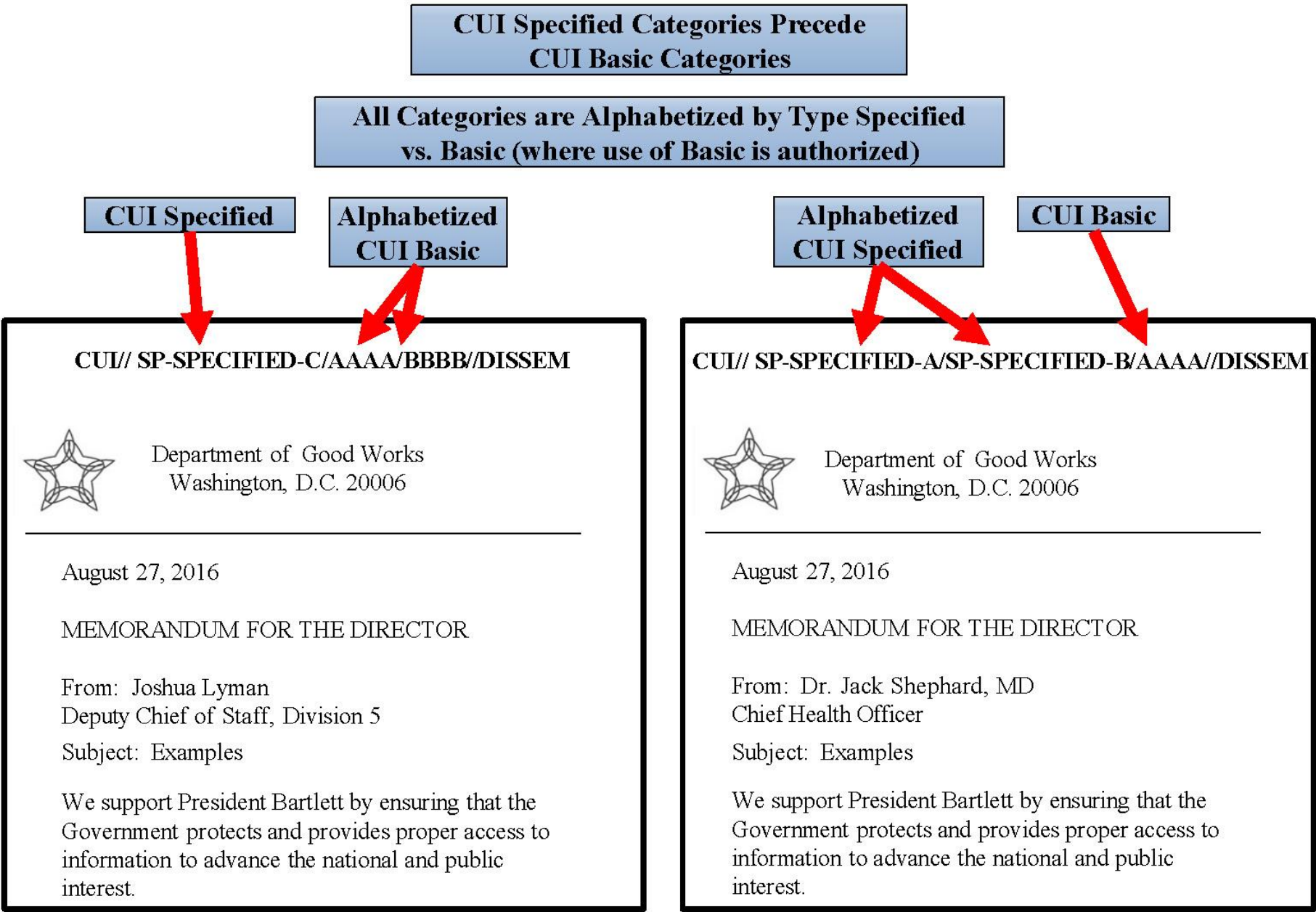
## Banner Markings (Multiple Category or Subcategory Marking)

CUI Specified Markings MUST precede CUI Basic Markings (where authorized for use by the agency head) in the CUI Banner. Consult your agency CUI policy for guidance on use of CUI Basic Category or Subcategory Markings.

CUI Category and Subcategory Markings MUST be alphabetized within CUI type (Basic or Specified).

Alphabetized Specified CUI categories and subcategories MUST precede alphabetized Basic CUI categories and subcategories.

Below are examples of CUI Banner Markings used in a document that contains both CUI Specified and CUI Basic



NOTE: The above examples use “AAAA” and “BBBB” as substitutes for CUI Basic Category and Subcategory Markings, “SP-SPECIFIED-X” as a substitute for a CUI Specified Category and Subcategory Markings, and “DISSEM” as a substitute for a Limited Dissemination Control Marking. Consult the CUI Registry for actual CUI markings.

Reference: 32 CFR 2002.20



# NIST 800-171

110 items across 14 categories

Small businesses are struggling to achieve compliance

Note that -171 applies to nonfederal systems (contractors) while 800-53 applies to federal systems

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "SP 800-171 Rev. 1" and displays the URL "https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final". The browser's address bar and tabs are visible at the top. Below the browser window, the NIST logo is prominently displayed on the left, and the "COMPUTER SECURITY RESOURCE CENTER" header is centered. The page content includes a green "PUBLICATIONS" button, the title "SP 800-171 Rev. 1", and the main heading "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". Social media icons for Facebook, Google+, and Twitter are present. The "Date Published" is listed as December 2016 (updated 02/20/2018), and "Supersedes" is noted as SP 800-171 Rev. 1 (December 2016 (Updated 11/28/2017)). The "Author(s)" section lists Ron Ross (NIST), Kelley Dempsey (NIST), Patrick Viscuso (NARA), Mark Riddle (NARA), and Gary Guissanie (IDA). An "Abstract" section begins with "The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and". On the right side, a "DOCUMENTATION" section lists links for "Publication" (SP 800-171 Rev. 1 (DOI) and Local Download) and "Supplemental Material" (CUI Plan of Action template (word), CUI SSP template (word), and Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 1 (xls)).

**NIST** Information Technology Laboratory  
**COMPUTER SECURITY RESOURCE CENTER**

**PUBLICATIONS**

**SP 800-171 Rev. 1**

**Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**

[f](#) [G+](#) [t](#)

**Date Published:** December 2016 (updated 02/20/2018)  
**Supersedes:** SP 800-171 Rev. 1 (December 2016 (Updated 11/28/2017))

**Author(s)**  
Ron Ross (NIST), Kelley Dempsey (NIST), Patrick Viscuso (NARA), Mark Riddle (NARA), Gary Guissanie (IDA)

**Abstract**  
The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and

**DOCUMENTATION**

**Publication:**  
[SP 800-171 Rev. 1 \(DOI\)](#)  
[Local Download](#)

**Supplemental Material:**  
[CUI Plan of Action template \(word\)](#)  
[CUI SSP template \(word\)](#)  
[Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 1 \(xls\)](#)

# GOVERNMENT UNIQUE ISSUES

## Contractor Perspective

Working with multiple agencies with different requirements

Different types of CUI on different contracts

Multiple frameworks depending on type of data/CUI

Government (DoD) is not accepting third party audits or certifications

Contracting Officer (CO or KO) might request POA&M and/or SSP as part of solicitation

SSP may be an evaluation factor for award

Reporting requirement

Medium level of assurance certificate and registration at <https://dibnet.dod.mil/portal/intranet/>



# GOVERNMENT UNIQUE ISSUES

## Government Perspective

Identifying CUI

Protecting CUI

Incorporating appropriate contract clauses

Evaluating and monitoring contractor compliance

# AUDITS & CERTIFICATION

US Government does not accept any audit report or third-party certification

**?** Q25: Will the DoD certify that a contractor is 100% compliant with NIST SP 800-171? Is a 3rd Party assessment of compliance required?

**A25:** No new oversight paradigm is created through this rule. If oversight related to these requirements is deemed necessary, it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract. The rule does not require "certification" of any kind, either by DoD or any other firm professing to provide compliance, assessment, or certification services for DoD or Federal contractors. Nor will DoD give any credence to 3rd party assessments or certifications – by signing the contract, the contractor agrees to comply with the terms of the contract. It is up to the contractor to determine that their systems meet the requirements.

Some companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.

Many primes require an audit or third-party verification



# ENGAGEMENT QUESTIONS FOR PRACTITIONERS

What is the nature of your engagement?

Consulting to help client achieve compliance?

Audit, review, or other attestation engagement?

Is the client doing this for themselves or satisfying the board, investors, or others?

Satisfying a contractual obligation with a prime?

Hoping to supply the report to the government?

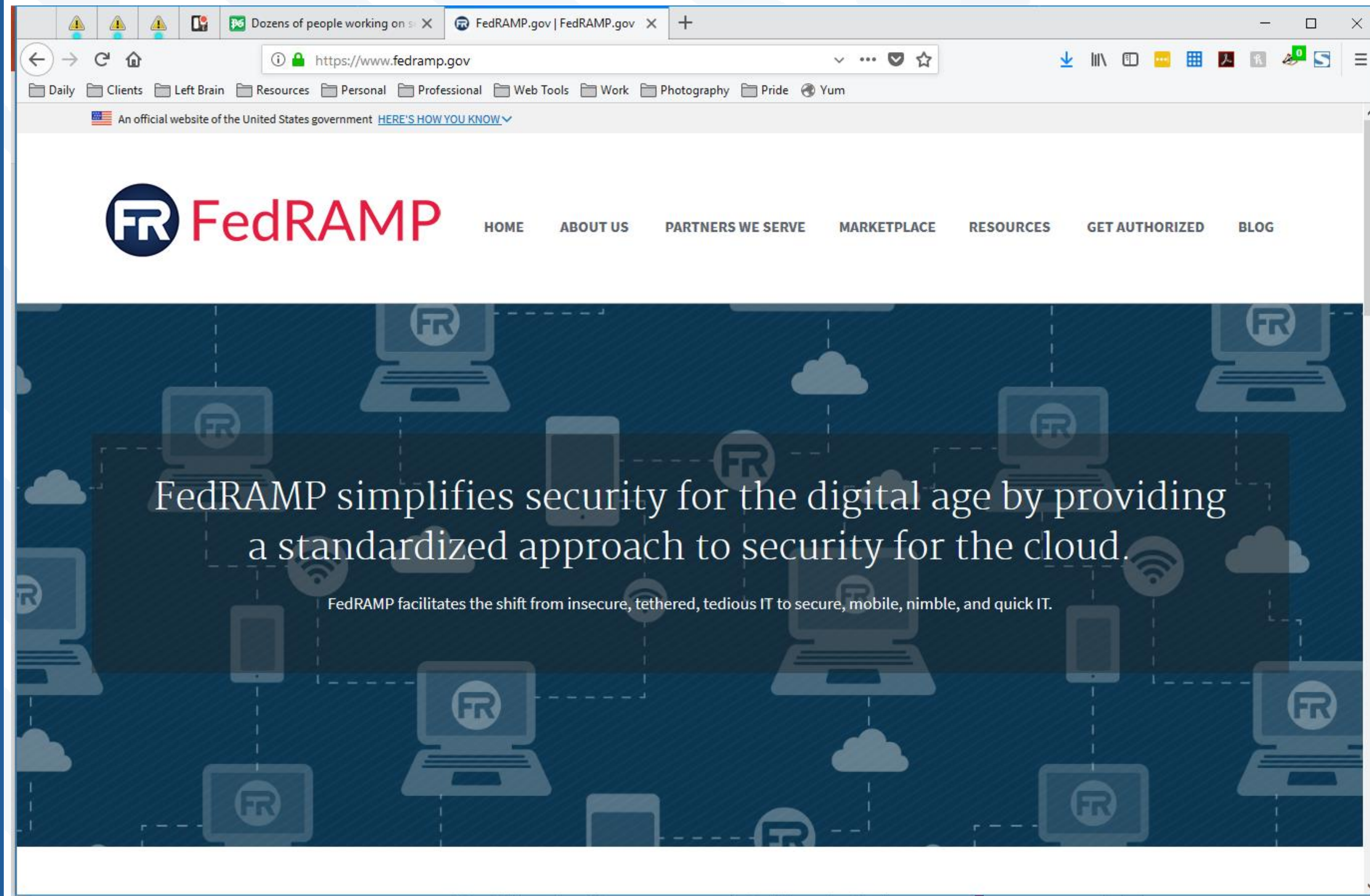
# FEDRAMP

“Do once, use many times”  
framework

Three-step process:

1. Security Assessment
2. Leveraging and Authorization
3. Ongoing Assessment and Authorization

Slightly misleading in that the FedRAMP stamp does not mean automatic approval for use within a specific agency





# MY TOP 10 TOOLS

1. Updates & Patches
2. Virus Protection
3. Passwords & Passphrases
4. Multifactor Authentication
5. VPN
6. Encryption
7. WiFi & Bluetooth
8. Backups & Cloud
9. Email
10. Social Media

# DOWNLOAD

Additional Resources

[www.leftbrainpro.com/infosec18](http://www.leftbrainpro.com/infosec18)





MIS|TI™ PRESENTS

# InfoSecWorld

Conference & Expo 2018

# THANK YOU

## PLEASE FILL OUT YOUR EVALUATIONS!

*Robert E. Jones*

*CPA, CPCM, NCMA Fellow*

*(614) 556-4415*

*Robert@LeftBrainPro.com*