DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Cloud Computing Security Requirements Guide (CC SRG)

Ron Rice
DISA Cyber Standards Branch (RE11)
May 2018

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

Agenda

- The Players
- Security Responsibility
- CC SRG Focus
- CC SRG and Mobility
- CC SRG Purpose
- History
- Impact levels
- DoD Provisional Authorization (PA)
- Mission Owner use of Cloud
- FedRAMP+
- Mission Owner Requirements
- Questions

The Players

- Commercial Cloud Service Providers (CSPs)
  - Offer Cloud Service Offerings (CSOs) to the public and/or government for a profit
  - Some CSPs offer DoD private CSOs

- DoD Cloud Service Providers
  - E.g., milCloud / milCloud2, and Component clouds
  - Offer Cloud Service Offerings (CSOs) to one or more DoD Components

- Mission Owners
  - DoD Components and sub-components that use CSOs
  - i.e., The “cloud customer” or CSP’s customer
  - Not the end user of what is in the cloud

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

Security Responsibility

SECURITY IN THE CLOUD

is a

SHARED RESPONSIBILITY

BETWEEN THE

CLOUD SERVICE PROVIDER

and the

MISSION OWNER

CC SRG Focus

- **The migration of DoD Applications and Services out of DoD owned and operated data centers to commercial cloud services while maintaining the security of, and the control over, all DoD data IAW DoD policies**
- **Why?**
  - **Enables DoD to keep better pace with technology advances**
    - Relies on the CSP’s tech refresh and software update processes
  - **If a service is virtualized there is more agility and flexibility to address demand and respond to security incidents**
    - Virtual machines are easy to kill if compromised and replace with a fresh image
  - **Migrating public facing web sites to IL2 CSOs reduces the attack surface of the DODIN**
  - **Enable the widest number of DoD mission owners to migrate their applications out of DoD data centers that are expensive to operate, while maintaining security and control of the data.**

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

CC SRG and Mobility

- CC SRG is not designed to support commercial mobile devices
  - Essentially these devices are typically connected to the Internet through a commercial cellular network
  - These devices typically expect cloud services for storage and applications to be connected to the Internet
  - Additional guidance and policy may need to be developed
- Waivers to current policy may be needed for mobility use cases for cloud services
- Commercial mobile device access to sensitive DoD data must be designed to protect that data

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

Cloud Computing SRG Purpose

- Provide guidance to DoD and non-DoD owned and operated Cloud Service Providers (CSPs) for hosting DoD information and systems
- Establish a basis on which DoD can assess the security posture of DoD and non-DoD CSP's Cloud Service Offerings (CSOs) and grant a DoD Provisional Authorization (PA) to host DoD information and systems
- Define the policies, requirements, and architectures for the use and implementation of DoD and non-DoD CSOs by DoD Mission Owners.
- Provide guidance to DoD Mission Owners, their Authorization Officials, and Security Control Assessors (SCAs) in planning and authorizing the use of a CSO.
- Provide guidance and a framework for the Cyber Defense of DoD Mission Owners' information and systems when using DoD and non-DoD CSOs
- Provide a basis through reciprocity for Mission Owners to grant Authorizations to Operate (ATOs)
- Enable the migration of DoD physical systems hosted in DoD NIPRNet Data Centers to DoD and non-DoD CSOs

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

Cloud Requirements History

- July 2012: DISA designated by DoD CIO as DoD Enterprise Cloud Service Broker (ECSB)
  - DISA begins to figure out how to address cyber security in the cloud
- May 2013: Cloud Security Model v1 Levels 1-2 Released by ECSB
- March 2014: Cloud Security Model v2.1 Levels 3-5 Released by ECSB
- NIST SP-800-53, FedRAMP, CNSSI 1253 Updated
- June 2014: DoD CIO Cloud Way Ahead Team Initiated
- December 2015: DoD CIO Released a memo RE:
  - "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services"
  - Eliminated the DoD Enterprise Cloud Service Broker
  - Left DISA in charge of security and connection requirements
- January 2015: Cloud Computing SRG v1r1 Released by DISA RME and DoD CIO
  - Updates guidance IAW NIST SP-800-53 rev4, FedRAMP (rev4 update), CNSSI 1253 (2014)
  - Rescinded CSM v2.1
  - Brought Cloud Computing Security guidance under the authority established by DoDI 8500.01 and DoDI 8510.01
- March 2016: Cloud Computing SRG v1r2 Released – A significant update
- March 2017: Cloud Computing SRG v1r3 Released – A significant update

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

Information Impact Levels

- **Information Impact Level - The combination of:**
  1) **The sensitivity of the information to be stored and/or processed in the cloud; and**
  2) **The potential impact of an event that results in the loss of confidentiality, integrity or availability of that information**

- **Cloud Security Model (CSM) defined 6 Information Impact Levels**

- **Cloud Computing SRG defines 4 Information Impact Levels**
  - **Levels 1 and 3 have been rolled up with the next higher level**
  - **Simplifies Impact Level selection and CSP capability matching**
  - **Levels designated as Level 2, 4, 5, 6 for consistency with the old CSM**

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

Information Impact Levels (cont'd)

- **Information Impact level 2:**
  - **Accommodates DoD information that has been approved for public release (Low confidentiality, Moderate Integrity)**
    - **i.e., public web sites**
    - **Includes some low confidentiality information requiring minimal access control**
- **Information Impact level 4:**
  - **Accommodates DoD Controlled Unclassified Information (CUI) (e.g., FOUO)**
- **Information Impact level 5:**
  - **Accommodates DoD CUI and National Security Systems (NSS)**
- **Information Impact level 6:**
  - **Accommodates DoD Classified Information up to SECRET**

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

DoD Provisional Authorization (PA)

- **DoD Provisional Authorizations are for Cloud Service Offerings, NOT CSPs**

- **Modeled after the Federal Risk and Authorization Management Program (FedRAMP) processes and Provisional ATO**

- **A DoD PA is an acknowledgement of risk based on an evaluation of the CSP’s CSO and the potential for risk introduced to DoD networks.**
  - **Acknowledges that the CSO is secure enough to process/store/transmit DoD information depending on its sensitivity as reflected by the Information Impact Level.**
  - **Provides a foundation that AOs responsible for mission applications must leverage in determining the overall risk to the missions/applications that are executed as part of a CSO toward providing their required Authorization to Operate (ATO).**

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

Security and Privacy Controls & FedRAMP+

- **FedRAMP Moderate Baseline serves as minimum set of Security Controls for all PAs**
- **FedRAMP High Baseline accepted as the basis for a IL4 PA without additional control assessment**
- **DoD FedRAMP+ Controls/Enhancements (C/CE) derived from a comparison of FedRAMP MBL and a CNSSI 1253 aggregate baseline for a categorization of Moderate Confidentiality (M), Moderate Integrity (M), Availability (x) (M-M-x)**
    - FedRAMP Baselines address availability
    - Additional availability addressed in the contract/SLA based on mission owner requirements
  - **CNSSI 1253 and FedRAMP baselines have the same basis**
    - CNSSI 1253 (2014) M-M-x Baseline
      - **NIST SP 800-53 rev4 Moderate Baseline PLUS CNSS tailored C/CEs**
    - FedRAMP, Moderate Baseline
      - **NIST SP 800-53 rev4 Moderate Baseline PLUS FedRAMP tailored C/CEs**
- **Nine additional FedRAMP+ C/CE to go from IL4 to IL5**
  - **With IL5 being limited to a DoD or Federal Government community**

- Vendors named within are approved or under contract to provide specified services to DISA or DOD

Security and Privacy Controls (cont'd)

- **Supplemental Control Requirements**
  - **CNSSI 1253 Privacy Overlay is invoked if PII/PHI is involved**
    - NIST SP 800-53 rev4 Privacy controls plus supplemental control guidance
    - CC SRG guidance is in development
  - **CNSSI 1253 Classified Information Overlay is invoked at Level 6**

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

Key Security Requirements Summary

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited “Public” Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI) ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

DoD Mission Owners

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

- When contracting for Non-DoD Off-Premises Cloud Services the Mission Owner is required to:
  - Use a CSP’s CSO that has a DoD PA at an impact level appropriate to the sensitivity of the DoD information that will be hosted (processed/stored/transmitted) by the CSO.
  - Comply with the Mission Owner requirements found in the CC SRG and any other DoD policy or requirements referenced
- Mission Owner Authorizing Officials (AOs) must provide an Authorization to Operate (ATO) for each application hosted in a CSO or each cloud services use case
  - The AO is to leverage the artifacts supporting the PA for the ATO determination
  - Assess the Mission Owner configured portion(s) of the CSO
  - Results in an informed acceptance of risk for DoD data in the cloud

Inheritance

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

- Remember Cloud security is a shared responsibility
- The Mission Owner inherits all C/CE that the CSO is responsible for depending on the service offering as reflected in their FedRMP and DoD PAs
  - E.g., all PE C/CE
- HOWEVER:
- The Mission Owner may be responsible for some the same C/CE
  - E.g., the CSP is responsible for access control to their CSO infrastructure; the Mission Owner is responsible for access control to what they build in the CSO (I/PaaS) and to the CSO console/portal; CM is another example
- The level of responsibility changes depending on how much control the Mission Owner has over the CSO environment.
  - I/PaaS = more shared responsibility
  - P/SaaS = less shared responsibility, BUT not eliminated.

Mission Owner Requirements - Highlights

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

- Categorize information IAW DoD policy (DoDI 8500.01/DoDI 8510.01/CNSSI 1253)
  - Select a Cloud Information Impact Level that matches that categorization
  - Consider Data location: on/off-premises; DoD private O&O vs Commercial O&O
  - Select a CSP with a PA that supports the Cloud Information Impact Level
- Establish access control and auditing IAW DoD Policy
  - CAC/PKI requirements are NOT waived for privileged users and user access to CUI
  - Includes CSP’s service ordering and service management portals/consoles
- Establish Cyber Defense (CD) services through one of the 23 DoD certified Cyber Security Service Providers (CSSP) for Mission Cyber Defense (MCD)
- Establish “private” connectivity to the CSP via a DoD CIO approved Cloud Access Point (CAP) for Information impact Levels 4 and 5
  - Various connectivity methods including DoD shared physical connections
  - CSP is not responsible for connecting to us… We as a customer connect to the CSP
- In IaaS/PaaS CSOs where the Mission Owner has control
  - Comply with all applicable SRGs/STIGs (OS, Application, Cloud, etc.)
  - Perform Mission Cyber Defense (MCD) functions

Mission Owner Requirements – Cont'd

* Vendors named within are approved or under contract to provide specified services to DISA or DOD

- **Protect Internet facing web sites and applications IAW DoD DMZ requirements**
  - **Whether IL2 or IL4; Whether public or restricted; Whether public or sensitive information**
  - **Includes providing proper encryption of data-in-transit for sensitive information**
  - **Includes providing proper boundary protections**
  - **Includes providing proper web site / application tiered architectures**
  - **Includes providing proper access control for sensitive information**
  - **Includes providing proper encryption of data-at-rest**
  - **Includes providing proper protections to thwart compromise of public web site computing resources**
    - Protect the integrity of the web site and public information disseminated
    - Prevent the use of this platform to attack / compromise other systems / applications / web sites, whether DoD owned or not

Contact Information & Questions

QUESTIONS

Contact info:
Ron Rice, CISSP, CCSP
DISA, Risk Management Executive Division
Cyber Standards Branch [RE 11]

Email: DISA STIG Customer Support Mailbox
disa.letterkenny.re.mbx.stig-customer-support-mailbox@mail.mil

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION