Software Assurance Tips

A product of the Software Assurance Tips Team[2]

Generated Friday 7th May, 2021

Jon Hood

Monday 5th April, 2021

1 COTS, GOTS, and NOTS software in RMF for the Army

When working as a government contractor security professional for a system that includes custom software, three different classes of software must be considered as part of the RMF process:

- COTS—Commercial Off-The-Shelf
- GOTS—Government Off-The-Shelf
- NOTS—Not Off-The-Shelf

A compliant Risk Management Framework (RMF) software list or Software Bill of Materials (S-BoM) manages the different approval paths for these types of software.

1.1 Identifying the Software

COTS software includes any software built for non-government, public activity. While COTS software implies a commercial aspect to the application, open-source and public domain software are also included in the definition of COTS software. While Shareware, Freeware, Adware, and as-is trial software are also COTS, they require explicit Army SISO approval on each system they're installed on and are not considered as part of this article.[3, 4–12.a.6] Open source components should be treated as any other COTS software for approval in a system. Each COTS component is listed in the system's software list, tracked by the change control board, and updates are subscribed to by a member of the security team. After listing the COTS software in the software list, its procurement (license costs and support information) are recorded in the system's Army Portfolio Management Solution (APMS) record. Remember that stand-alone COTS software should never be placed alone into APMS. Doing so will cause the APMS records to indicate that the Army is paying multiple times for software and has been used as an attempt to inflate budgets. The procurement cost for the software is dependent upon the system implementing the software and is recorded in each implementing system's APMS record.

GOTS software is software that is not sold commercially or provided publicly. It is software created for or owned by a government agency. This doesn't mean that commercial/contractor providers don't own the software. GOTS software falls into three sub-categories:

1. *GOTS software created by direction of the government for a particular purpose.* This software is then owned by the public domain (owned by the taxpayers) and is generally easy to share with other government agencies or protect at appropriate levels.
2. *GOTS software created by a company or individual for fulfilling a government-directed duty.* When the government gives direction to create software, this should include contract language to direct the company creating it. By default, the restrictions of DFARS, specifically 48 CFR § 252.227-7014, apply to the software.
3. *Software assigned to government ownership.* When software is created by the government, it falls under non-copyrighted public-domain software. When a copyright holder assigns copyright to the US, the software is treated as public-domain, but the attribution of copyright assignment is retained for non-repudiation purposes. You will see something like, "Copyright © 2020 Jon Hood; assigned to US government on 8/9/2020" in the source files. There must be a valid previous copyright holder to assign the copyright to the government.

1.2 Assessing the Software

COTS products can be assessed in multiple ways:

- If the COTS product has an official Security Technical Implementation Guide (STIG) or Security Requirements Guide (SRG), it is approved by DISA and reciprocity allows its use throughout the DoD. The software is assessed in the implementing environment by applying the STIG/SRG.

- If the COTS software has no STIG or SRG, Software Assurance (SwA) is performed on the product.
  - If the software has source code available, it is scanned using static source analysis. The Application Security and Development (ASD) STIG is filled out and supplied, along with the SA-11* controls.
  - If the software does not have source code and the product is being assessed for mission support functionality, a dynamic binary analysis scan is performed. SA-11* controls are filled out and a partial STIG report is provided.
  - If the software is being used in a mission essential or mission critical environment, particularly on tactical systems, a static binary analysis with reverse engineering is recommended. The ASD STIG and any relevant SA-11* controls are completed.

When filling out the ASD STIG for COTS software, several of the checks deal with a development environment that is not geared towards developing the software for a government environment. Checks that pertain to development processes and requirements can be marked as Not Applicable because the COTS software has already been selected because it fulfills a requirements for a particular mission. If a mission dictates new requirements that require custom development, that development should consider falling under GOTS.

For GOTS software, the software is first assessed for compliance from a legal perspective:

- Is the software in the public domain with source code available?
- Does the software meet the definition of "computer software" under GOTS Fdederal Acquisition Regulation (FAR) definitions?

If the software is GOTS, you will have the entirety of instructions for how to build the software. This is the legal definition of GOTS. If you cannot build the software or are not provided the source code, the software does not meet the definition of GOTS computer software per the FAR.

Once the software has been identified as GOTS, the ASD STIG is evaluated and any relevant SA-11 controls are tailored in to the RMF control selection.

There is a final class of software that pretends to be GOTS but does not provide source code or build instructions. This is considered "NOTS" software. This is often proprietary or IP-protected code, written at taxpayer expense, and not provided back to the public. Instead, contractors and civilians attempt to re-sell the software repeatedly back to the taxpayers who funded its development. This is why the DFARS regulations under 48 CFR § 252.227-7014 were written. Note the very definition of computer software to fall under DFARS's definition of restricted rights GOTS software (emphasis added): "Computer software means computer programs, **source code**, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer databases or computer software documentation." By legal definition, you will have the source code and everything you need to rebuild the source code to a working product if the software claims to be GOTS. A contractor may then say, "Well, we'll just say that the software is COTS then." Now, that contractor must abide by the FAR definitions of commercial software (FAR 2.101) and Non-Developmental Items. The software must be:

> (i) A commercial item...;
> (ii) Sold in substantial quantities in the commercial marketplace; and
> (iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace;...[1]

A piece of software that is not sold in a public, commercial marketplace is not COTS. Likewise, software that does not provide source code and build instructions is not GOTS. These software packages are non-COTS, non-GOTS, and simply "not off-the-shelf" NOTS software that must have explicit AO approval and be tracked using non-FAR-compliant acquisition processes.

Nevertheless, there is a non-trivial amount of NOTS software that is in use by the Army. Our recommendation: perform a best-effort SwA scan, but also mark high-risk findings against the following checklists:

- On the ASD STIG, mark SV-222658r508029_rule (as of ASD V5R1) as a finding with the comment, "The support contract does not meet the requirements of COTS, nor does the application meet the definition of Computer Software for GOTS. COTS software must be procured through proper acquisition channels (`https://www.acquisition.gov/content/2101-definitions#i1125359`), and GOTS computer software must provide source code and build instructions (48 CFR § 252.227-7014)."
- Tailor in (if not already in the baseline) and mark as NON-COMPLIANT RMF control SA-22, CCI-3376 with the comment, "A software package does not provide either COTS or GOTS support mechanisms."
- Tailor in (if not already in the baseline) and mark as NON-COMPLIANT RMF control SA-4 (6), CCI-631 with the comment, "The system employs software that is not COTS or GOTS."

Note that RMF CCI-631 requires your software solutions to be either COTS or GOTS: "The organization employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted." By attaching a finding to CCI-631, the program must include the finding in their POA&M for tracking and obtain AO approval for the non-compliant software.

References

[1] GSA. *Federal Acuisition Regulation. Definitions*. Department of Defense. 2019. URL: https://www.acquisition.gov/far/2.101.

[2] Jon Hood, ed. *SwATips*. https://www.SwATips.com/.

[3] HQDA. *Army Regulation 25–2. Information Management: Information Assurance*. Department of the Army. Washington, DC, USA, 2019. URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN17503_AR25_2_Admin_FINAL.pdf.