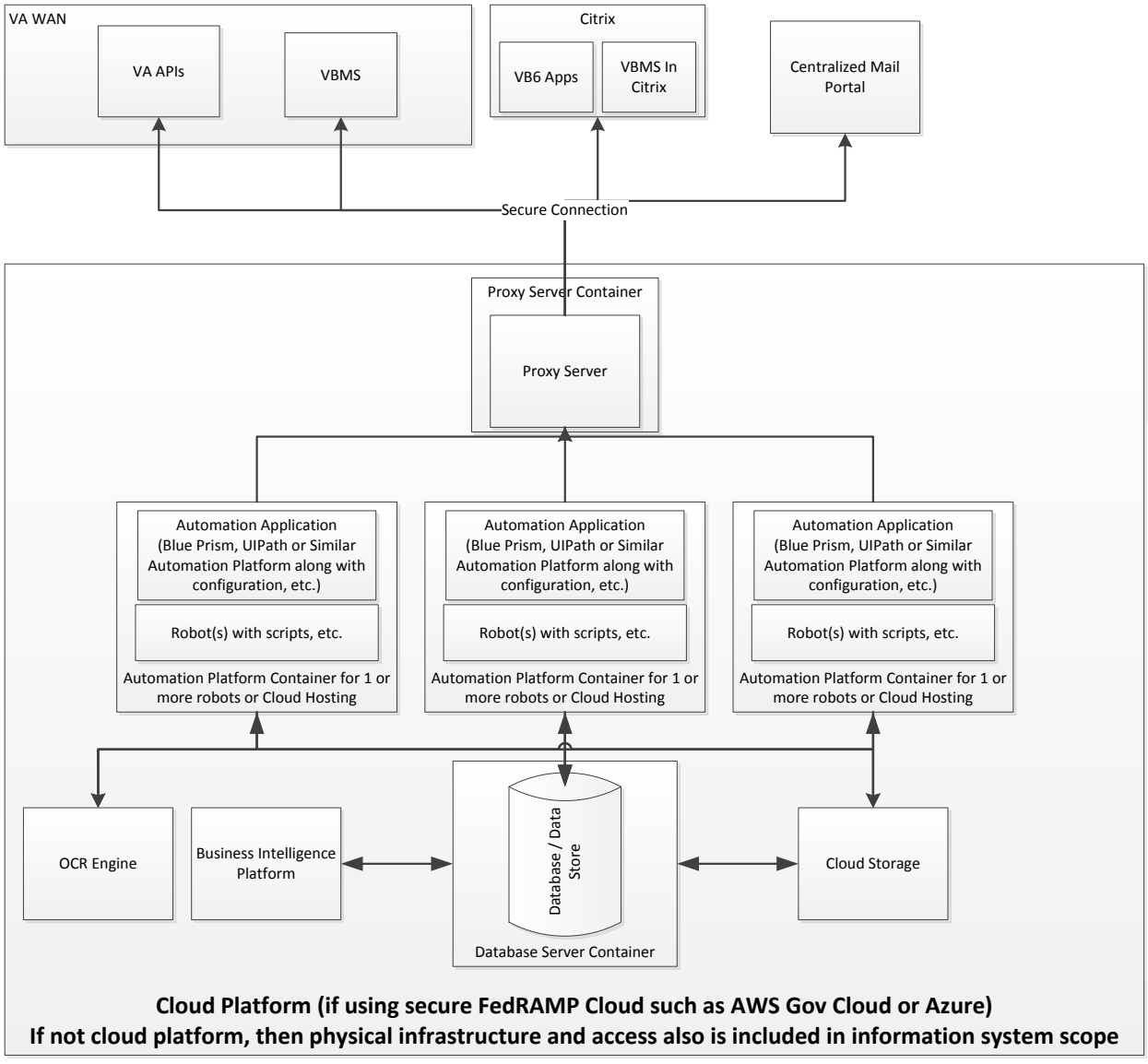
A Basic Guide to the VA Authority to Operate (ATO) and Other Security Processes

VBA makes no representations about the below guide being inclusive or totally accurate. It is intended to discuss at a practical level what the ATO and other security processes entail.

All VA information systems, including the system of the Contractor, must receive ATOs and complete other security requirements. This is a requirement to appropriately ensure the sensitive information of Veterans is appropriately protected. This guide describes the basic process and actions needed to get to an ATO and complete these other processes.

Information Systems

Let's talk for a minute about what we mean by an information system. For the purposes of this contract for automation, we assume the Contractor will have something that vaguely looks like this:

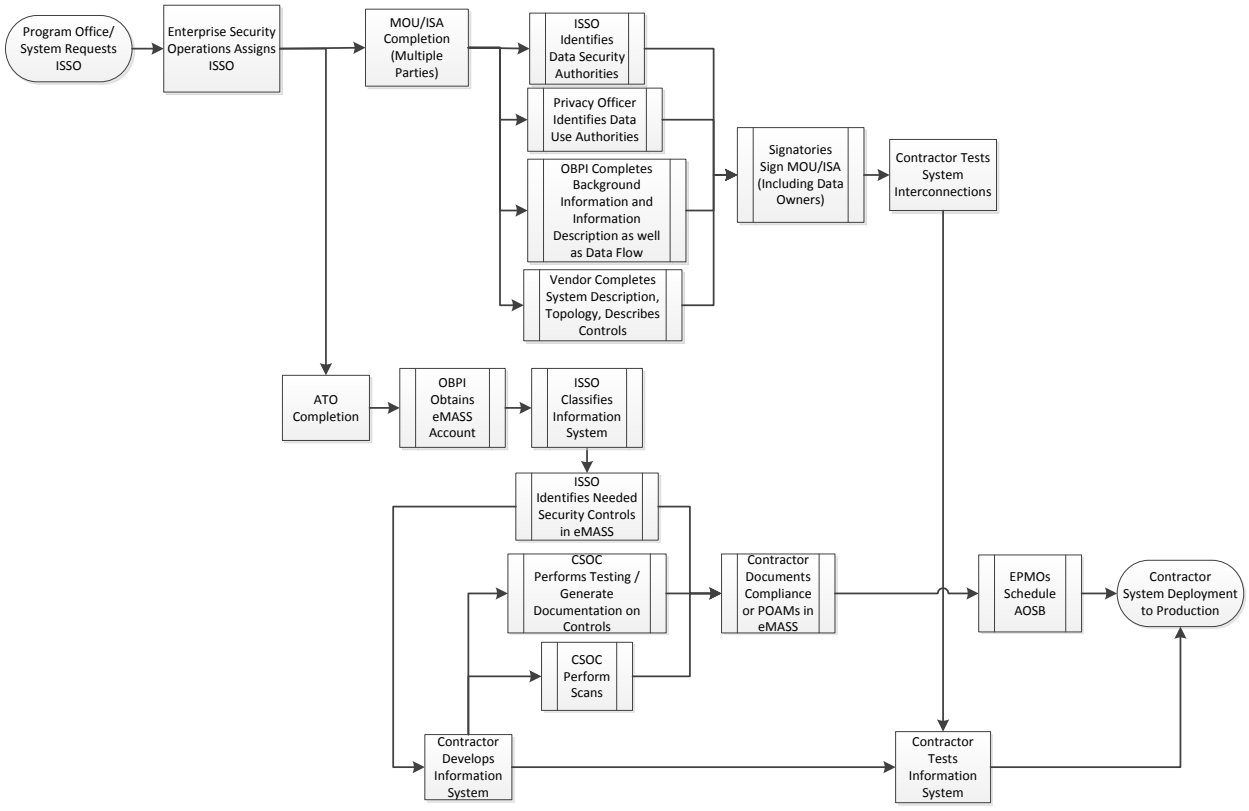


Essentially, everything within the Contractor's cloud platform, including the Contractor's accesses to their cloud platform and items within (containers, OSes, configurations, files and data), as well as the Contractor's interfaces to VA count as a part of the Contractor's information system.

Why do we obtain ATOs and complete the other requirements?

VA's ATO process certifies an information system has the appropriate ***security controls*** in place to prevent a security breach. The needed controls are dictated by an information system's classification, which correlates to the potential impact of a potential system security breach with low, moderate, and high impact classifications possible. Because the Contractor's system will have access to Privacy Act protected information including personally identifiable information (PII) and because VBA relies on the systems the Contractor is accessing perform mission-essential functions, the Contractor's system classification will likely be **Moderate**. We also complete other requirements, most notably creating a Memorandum of Agreement/Interconnection Security Agreement (MOU/ISA). We create an MOU/ISA as an additional safeguard surrounding the data being transferred by VA to the Contractor and by going through that process ensure 1) the data is appropriate to share (in this case, it is), and that the Contractor understands the various controls in place that are contingent to receive the data.

What do the security processes look like?



The above process flow captures an extremely high-level, slightly fuzzy overview of what the ATO and MOU/ISA processes look like. Both begin with the program office, in this case VBA's Office of Business Process Integration (OBPI). OBPI has begun laying the security groundwork for the seed task order even as offerors are completing their proposals. To this end, OBPI has worked with Enterprise Security to have an Information Systems Security Officer (ISSO) assigned who will help the Contractor through the

process and validate the Contractor has appropriately satisfied the required security controls. This ISSO has been assigned. Next, following the ISSO assignment, the process branches slightly into ATO and MOU/ISA paths.

The MOU/ISA path is really about the completion of and concurrence on a document. However, this document is dependent both on the security controls elaborated in the ATO process and on the Contractor's own system design and high-level network topology depicting the Contractor's information system. The MOU/ISA also includes portions surrounding the data being shared (in this case, Veteran/claimant applications for benefits and various documents as well as PII, etc.) and VBA's ability to share it (which are in this case covered under the routine uses of the Privacy Act since the Contractor is an agent of VA). Once these various aspects of the document are completed, they will be routed for Privacy Officer, ISSO and line of business (in this case Compensation Service and Pension and Fiduciary Service) signatures as well as the signature of the Contractor (who is a party to the agreement). **Once an MOU/ISA is complete, the Contractor may begin testing and connecting to VBA's test environments and testing their solution.**

The ATO path on the other hand is all about documenting controls and performing various testing. Once the ISSO has been assigned, he/she will work to identify the applicable security controls as outlined in VA Handbook 6500, Appendix F. VBA assumes the ISSO will determine the controls for a moderate categorization are needed since the Contractor will be accessing PII, Controlled Unclassified Information (CUI) etc. For many of these controls, Handbook 6500 already contains the relevant implementation at the low, moderate and high implementation. Where the controls are left up to the system owner, the Contractor will work with OBPI to determine the appropriate controls required. Please see VA Handbook 6500, Appendix F for a complete listing (starting on page 97) of these controls and the baselines. Attachments 1, 2 and 3 are also handy here as they contain practical descriptions of these controls. Many of these controls and their baselines are extremely common sense, such as CM-3, for instance, which essentially says the Contractor must have internal change control processes that prevent them from making and deploying changes without a documented, controlled process. For each of the controls listed in the Enterprise Mission Assurance Support Service eMASS, a portal where the Contractor will complete the ATO process, the Contractor will need to provide evidence. This could include test results, documentation, screenshots, etc. – essentially the Contractor will be proving to VA they are compliant – for change control (as an example only), that might include a change control board structure, with minutes, etc. as well as proceedings about deployments.

Even as the Contractor is documenting their compliance with the controls, the Contractor will also have to open up their systems to three specific types of testing that go beyond the Contractor's own assertions. These are the Web Application Security Assessment (WASA) test – a manual penetration test, NESSUS scan, and the Database scan and Penetration (recurring and automated) testing. These scans attempt to identify various vulnerabilities in the Contractor's system to ensure they cannot easily be compromised.

In the event there are findings either related to the security controls or to the testing, the Contractor does NOT necessarily have to remediate all findings prior to deployment to production. Rather, the Contractor must work with the ISSO to document a plan of actions and milestones (POAM) on when the findings will be corrected. It is highly likely the Contractor will have multiple findings the first time through the ATO process and this is expected – so long as no findings are highly egregious or so long as

the Contractor has risk mitigations in place, findings will not stop the Contractor from deploying to production.

Once the various scans are complete and the security controls are validated, the Contractor will work with the Enterprise Program Management Office to provide an Authorizing Official Security Briefing which, if the Contractor has appropriately participated in the ATO process and established any POAMs needed, will result in a temporary ATO of varying length, with the intent the Contractor will be given conditional deployment approval while correcting/remediating issues.

ATOs are Not Permanent

The Contractor should assume the ATO process is continuous, not a specific way-station on the path to deployment. Almost all VA ATOs come with specific time-limited elements and typically, the maximum length of an ATO issued is only a year. The Contractor likely will not get a year initially, but only a 30-day ATO, with progress expected on POAMs within the 30-day cycle. ATOs are not merely continuous because work remains to be done, but also because the definition of secure continues to evolve at a high level – new vulnerabilities are identified daily in both public and private sector systems and because the Contractor's system will also continue to evolve. As the Contractor makes changes to the system, these changes will also need to be reflected in their eMASS entries and documentation related to security controls.