Business Applications Solution (BAS) Program
Table Talk

UNITED STATES DEPARTMENT OF COMMERCE
OFFICE OF FINANCIAL MANAGEMENT
AGENDA

01 Software as a Service
02 Hosting Platform
03 Security
04 Getting Involved
BAS PROGRAM TABLE TALK

PRESENTERS

Andy Blumenthal  
**BAS Deputy PM**

Rick Murray  
**AFS BAS Project Manager**

Sai Pakkam  
**AFS BAS Technical Architecture Lead**

Michelle Woolfolk  
**AFS BAS Security Program Lead**

Jon Ford  
**AFS BAS Security Lead**
Cloud Computing Service Models

- **Infrastructure as a Service (IaaS)** - Most basic cloud service model. Providers offer infrastructure services - compute services (physical or virtual), networks, storage and firewall.

- **Platform as a Service (PaaS)** - Providers offer a computing platform, which includes the IaaS model along with the operating systems, web servers, and security services.

- **SaaS** - Most comprehensive cloud service model. Providers offer all the aspects included in the PaaS platform, in addition to installation and management of application software.
BAS PROGRAM TABLE TALK

COMMERCE BENEFITS OF SaaS

**SaaS Benefits**

**Flexibility**
- Ability to rapidly scale infrastructure to meet changing business needs
- Access to latest technology to allow for continuous innovation

**Reduce Risks**
- Federal Risk and Authorization Management Program (FedRAMP) compliant systems
- State of the art data centers
- Automation and scheduled upgrades
- Shorter deployment timelines for new features

**Reliability**
- Always on latest version of software
- Managed Service with operation teams monitoring system for system performance and availability

**Cost Avoidance**
- Reduction in on-premise applications to deploy, implement, or manage
- Allows for focus on business outcomes versus IT maintenance

**Security**
- SaaS Platform
- SaaS

BAS PROGRAM TABLE TALK
HOSTING PLATFORM MODEL

BAS Solution

- AFS manages BAS Portal (ServiceNow) and BAS Platform
- AFS augments and maintains the PaaS and IaaS components for a standardized solution across Commerce
- AFS and providers jointly perform security services across all BAS components

BAS delivered and maintained at Commerce as SaaS
Authorization To Operate (ATO) process - extremely similar for systems leveraging FedRAMP packages – but with several key differences.

• Prior to FedRAMP, government systems requirements for ATO:
  – Review individual service provider packages, develop processes, reports, Interconnection Security Agreement (ISA) / Service Level Agreements (SLAs)
  – Needed for each tenant for all providers

• With FedRAMP, Cloud Service Providers (CSPs) requirements:
  – Standard control implementations and authorizations
  – Authorize Once, Use Many approach
FedRAMP Authorized CSPs still provides a high-level assurance to federal systems

- Reduces amount of controls to implement (IaaS > PaaS > SaaS)
- Does not eliminate need for the federal ATO process
- BAS is still responsible, either fully or shared, for the implementation of 168 controls
  - Independently assessed
  - Receives ATO from responsible Department or Agency

DOC requires all cloud systems be FedRAMP Compliant

- Systems with PII need to comply with the OPOG* Privacy Overlay
- BAS will implement additional controls outside of a normal NIST 800-53 Rev. 4 Moderate control baseline and develop additional processes and requirements

*BAS Control Breakdown

- Total: 391
- FedRAMP Provided Controls: 226
- BAS Responsible Controls: 168
- BAS Solutions: 98
- NIST 800-53 Rev 4, Privacy: 27
- DOC OPOG Privacy Overlay: 43

*Office of Privacy and Open Government
<table>
<thead>
<tr>
<th>Solution</th>
<th>FedRAMP Package</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Data Warehouse / Business Intelligence (EDW/BI)</td>
<td>Accenture Insights Platform (AIP) Platform as a Service (PaaS) [JAB P-ATO]</td>
<td>Enterprise Data Warehouse/Business Intelligence and Ad Hoc Reporting</td>
</tr>
<tr>
<td>ServiceNow</td>
<td>ServiceNow Government Community Cloud Software as a Service (SaaS) [JAB- ATO]</td>
<td>BAS ITSM and Future Single Sign-On (SSO) Portal</td>
</tr>
<tr>
<td>Xtended Detection and Response (XDR)</td>
<td>Accenture XDR for Government Software as a Service (SaaS) [Agency ATO]</td>
<td>Managed Security Detection, Alerting, Reporting &amp; Analytics</td>
</tr>
</tbody>
</table>

**PRE-ATO**
- REVIEW FEDRAMP PACKAGES
- DEVELOP SECURITY DOCUMENTATION
- COLLECT EVIDENCE TO SUPPORT CONTROL IMPLEMENTATION
- DOCUMENT RISK ACCEPTANCES AND POAMS

APRIL 2020 – DECEMBER 2020*

**ASSESSMENT AND ATO**
- COALFIRE WILL CONDUCT ASSESSMENT AND PEN TEST
- COMPILATE ATO PACKAGE
- SUBMIT DOCUMENTATION TO FEDRAMP

JANUARY 2021 – APRIL 2021*

**POST-ATO**
- MOVE TO CONTINUOUS MONITORING PHASE
- PRODUCE METRICS AND DASHBOARD REPORTS

APRIL 2021 – BEYOND*

*Proposed Timeline; Subject to Change
• Real-time, managed security service for event management, alerting, security monitoring, and threat intelligences
• Helps identify suspicious behavior and aligns the solution to specific needs
• Using industry-leading tools, will allow BAS to meet or exceed compliance standards and requirements through rapid response and remediation
• Will provide a holistic view across all BAS solutions and assist the BAS Security team, DOC, and CSPs to review audit logs and alerts and respond in a timely fashion

At a Glance:
• FedRAMP authorized (moderate)
• SOC is staffed 24x7x365
• Customer Portal provides real-time visibility
• Real-time updates of security posture and core metrics
• Overview of open investigations
• Detailed look at security posture with suggested improvements
• Contact information and form
• Questions/Concerns/Feedback? Want to be involved? Contact BAS Project:
  BASProject@doc.gov

• Need more information? Visit us online at:
  https://www.commerce.gov/ofm/bas-homepage/business-applications-solution-bas