ISPG DevSecOps Overview
GOAL: Build Security into DevOps

Mission
- ✓ Stay Secure Every Sprint
- ✓ Expedite ATO Process

Approach
- ✓ Open Source
- ✓ Automation

Objective
- ✓ Publish Best Practices
- ✓ Incorporate ISPG Policy

Established Capabilities

Open Source Community

https://github.com/mitre*

ACT Support

Aid ISPG ACT team in deploying these tools for security assessments

Best Practices

DevSecOps Checklist + Confluence Pages

Training for DevOps Teams

Testing Tools & Content

- **36** CMS InSpec security profiles
  https://github.com/orgs/CMSgov/teams/ispg/repositories

- InSpec_tools to convert STIG/CIS standards to profiles *(>7200 downloads)*

Visualization Tools

- Heimdall-lite + Server *(>9000 downloads)*

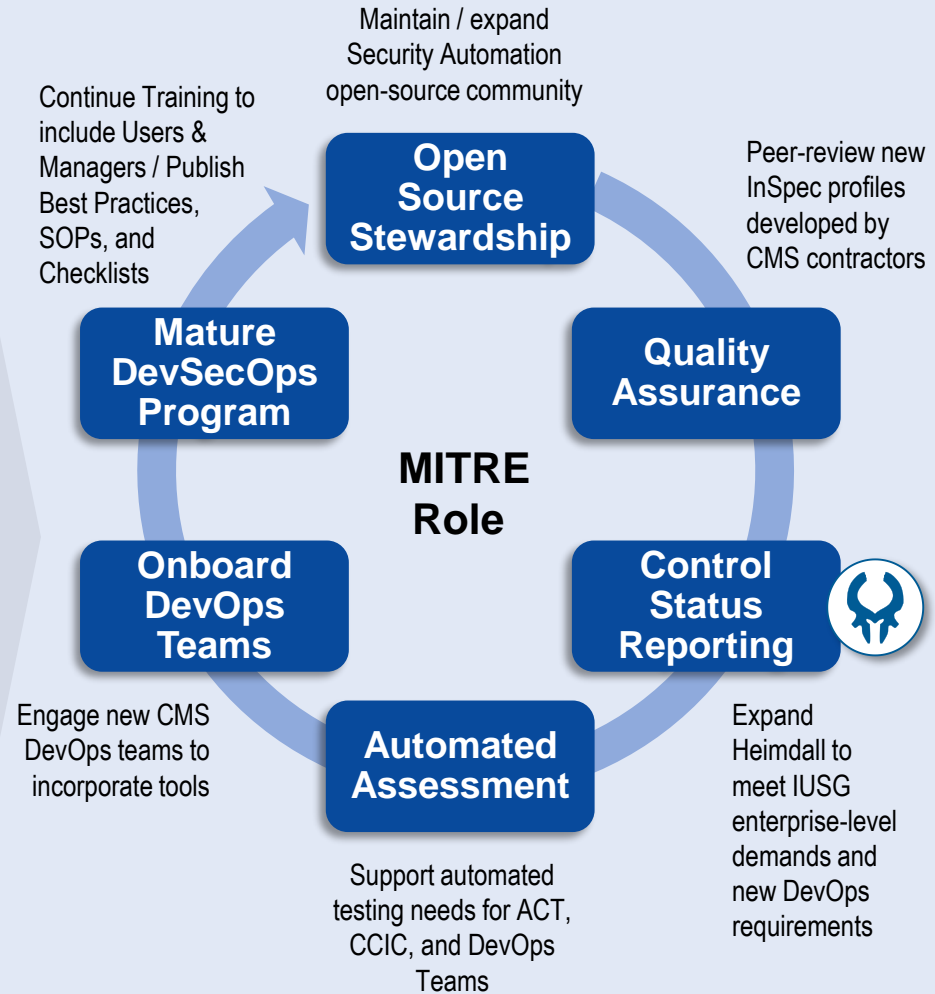- Heimdall_tools to convert static and dynamic security tool output to Heimdall format *(1000 downloads)*

DevOps Pilots

- IUSG
- BCDA
- CFACTS
- T-MSIS
- IDM
- MACFIN
- Lewin Group

7 classes provided, including DHS staff and contractors

48 CMS contractors trained to develop InSpec profiles
Basic Class + Advanced Class

MITRE Role

Continue Training to include Users & Managers / Publish Best Practices, SOPs, and Checklists

Maintain / expand Security Automation open-source community

Peer-review new InSpec profiles developed by CMS contractors

Open Source Stewardship

Mature DevSecOps Program

Quality Assurance

Onboard DevOps Teams

Control Status Reporting

Automated Assessment

Engage new CMS DevOps teams to incorporate tools

Support automated testing needs for ACT, CCIC, and DevOps Teams

Expand Heimdall to meet IUSG enterprise-level demands and new DevOps requirements

MITRE helped establish and is supporting all of these ISPG DevSecOps initiatives

April 2020 Update