**GSAW 2019 Tutorial D:**

Improving Security of Ground System Software

**Length:** Half day

**Overview:**
**Tutorial Outline:**

- Getting on the Same Page with Ground Systems
  - Defining ground systems @ NASA and in DoD
- Threat Landscape
- What is SW in a Ground System?
- SW Security is Required but Barriers Exist
- What is FISMA / NIST's role in SW security
- Approach for Secure and Resilient Software
  - System Threat Modeling
  - Sample Process for Developing Secure Software
    - System Security Threat Understanding
    - Develop Security Strategy
    - System Security Plan
    - Secure SW Development (COTS/FOSS/Supply Chain)
  - Software Threat Modeling
  - Alphabet Soup – VA, SCA, OA, CWE, CVE, CWSS
- Ground Software Examples and Metrics
- Near Team Goals and What to do Now?
- Trends and Lessons Learned
- Future: DevSecOps and Cloud

**Instructor:** Brandon Bailey, TMC Technologies

**Biography:**
**Brandon Bailey** is currently the Chief Technology Officer and Cyber Division Manager for TMC Technologies. Brandon has been supporting NASA and DoD organizations for over 13 years in the test and evaluation field with specialization in cybersecurity. Brandon has experience testing in both the intelligence and civil space arena but recently Brandon's work at National Aeronautics and Space Administration (NASA)'s Independent Verification and Validation Program involved building and managing a software testing and research laboratory as well as leading the information assurance and cybersecurity activities as they relate to NASA's space and ground missions. These efforts resulted in improving the security for the mission segments within NASA's enterprise which includes: vulnerability assessments, infusing secure coding principles, counteracting the threat landscape by infusing security analyses in the standard IV&V workflow and working within the CCSDS security working group to develop international security standards.

**Description of Intended Students and Prerequisites:**
Have understanding of basic software development. The audience are developers and managers for developers. Will be a mix of detailed technical content as well as concepts for management.

**What can Attendees Expect to Learn:**
An estimated 84% of all security breaches are application-related, ***not firewall violations***. To what extent is your organization focused on addressing security issues in its software? Software plays a critical role in mission success, and software similarly plays a role in mission security. However, software can introduce vulnerabilities to the system, such as use of a COTS product that has a

backdoor, or a hole in the security of the system deliberately left in place by designers or maintainers. The motivations for such holes are not always sinister, but can provide a means for malicious intrusion into the mission. Students will learn an approach to securing ground software within the context of federal information systems. Federal requirements, coding standards, tool usage will be discussed as part of the solution to securing software.