



---

# ***NDIA MDA SBIR Industry Day***

***Information Assurance Research Area***

***Ms. Susan Todd***

***MDA/DOS***



# Agenda

---

- Research Area Objectives
- List of Topics
- Topic Overview
- Questions



# Research Area Scope and Objectives

---

- The Ballistic Missile Defense System (BMDS) contains a diverse set of components requiring protection from a wide array of threats.
- The purpose of the Information Assurance (IA) Research Area is to research and develop technologies and tools that are designed to enhance the security posture of the BMDS



# Topics

---

- Real-time Application Security in a Communications Network
- Power Solutions for Integrated Anti-Tamper Technologies
- Ballistic Missile Defense Anti-Tamper Penalty and Response Capabilities



# Real-time Application Security in a Communications Network

---

## OBJECTIVE:

–Develop and demonstrate innovative solutions to the problem of application security within the context of Ballistic Missile Defense System (BMDS).

## DESCRIPTION:

–Within the context of a distributed, real-time information assurance management platform, there is a need for a process with the ability to interrogate user applications for security vulnerabilities, monitor them for attack while in operation and track the status of improvements to correct the vulnerabilities.. The topic author is looking for innovative solutions that will automate the latest in application penetration testing within the BMDS. The solution should be able to operate in both a test and operational state. During operational state the goal should be on monitoring for live attack directly on the running software applications. During test state the solution should focus on more in-depth application penetration testing. Both solution states should provide as an output recommended code changes.

–Innovative solutions should include but not be limited to:

- Real-time software application penetration testing capability
- Graphical security level state information
- Recommendations for improvements with complexity factor and projected gain as reported by reduced security risk level
- Status of improvements to date

## PHASE I:

-Analyze, design, and conduct proof-of-principle demonstrations of methods for real-time application security systems that provide insight into this aspect of the overall comprehensive situational awareness of the Information Assurance state of the BMDS and its components.



# Power Solutions for Integrated Anti-Tamper Technologies

---

## OBJECTIVE:

–Develop and implement continuous power enhancements for Anti-Tamper (AT) technology for the protection of critical technology against exploitation.

## DESCRIPTION:

- Add longevity to critical technology by deterring efforts to reverse-engineer, exploit, or develop countermeasures against a system or component.
- Identify methods to respond to tamper events that may lead to unauthorized access to CPI.
- Improve power solutions for use when providing power for the operation of Anti-Tamper techniques to protect weapon systems. This includes the development of power sources and the innovative implementation of COTS power sources for AT applications.
- Focus on developing enhanced power solutions that provide sufficient power to AT techniques and technologies for initiating and accomplishing protective actions. The power solution(s) need to be independent, small, light weight, and covert to protect from tampering.
- Results should address:
  - Significant challenges associated with implementing AT utilizing current available power sources
  - Power integration as a seamless part of AT integration into the weapons system.

## PHASE I:

-The contractor shall develop the conceptual framework for new and innovative AT power options. The contractor will also perform an analysis and limited bench level testing for an understanding of the power requirements and provide metrics to be used to demonstrate the value of these enhancements.



# Ballistic Missile Defense Anti-Tamper Penalty and Response Capabilities

---

## OBJECTIVE:

–Develop and implement new innovative anti-tamper (AT) response and penalty protection technology for the protection of critical technology against exploitation.

## DESCRIPTION:

- Add longevity to critical technology by deterring efforts to reverse-engineer, exploit, or develop countermeasures against a system or component.
- Identify methods to respond to tamper events that may lead to unauthorized access to CPI.
- Response and penalty methodologies may include, but are not limited to:
  - Destruction of CPI
  - Surreptitious configuration alteration
  - Irreversibly degraded performance
  - Commensurate response to match attack

## PHASE I:

-The contractor shall develop the conceptual framework for new and innovative AT protection technology or technique that is integrated with, or tailorable to, the CPI being protected. The contractor will also perform an analysis and limited bench level testing for an understanding of the new and innovative response protection technology.