



**engineering** systems solutions

**Information Assurance Overview**

**real** solutions for the real **world**

# Briefing Objective



The purpose of this briefing is to provide an overview of Engineering Systems Solutions (ESS) and our Information Assurance (IA) capabilities. As a Service-Disabled Veteran-Owned Business, ESS can provide many value added IA and IT enterprise solutions that augment and enhance our customers' capabilities, as well as our teaming partners' offerings, across the Federal Government, Department of Defense, Intelligence Community and niche industry markets.



# Corporate Profile



- Value-added provider of professional IT, IA and Web Development services
- Also specializing in:
  - Systems Engineering and Integration
  - Digital Forensics
  - Modeling and Simulation
  - Product Lifecycle Management
- Founded in 1993 as an 8(a) Service Disabled Veteran-Owned Small Business. Graduated from 8(a) in 2005.
- Over 120 associates
  - 70% hold government clearances that are TS or higher
  - Many possess specialized degrees and IA/IT-related certifications
  - Experienced Program Management professionals
- ISO 9001:2000 Registered



# Locations



- Frederick, MD (HQ)
- Ft. Detrick, MD
- Andrews AFB, MD
- Ft. Meade, MD
- St. Louis, MO
- Orlando, FL
- Pentagon
- Huntsville, AL
- Langley, VA
- Colorado Springs, CO
- Dayton, OH
- Ramstein AFB, Germany
- Rosslyn, VA
- Washington, DC



# Information Assurance (IA) Capabilities and Services



- IA Overview
- IA Relevancy – Evolution of Threats
- ESS IA Capabilities
  - ESS IA Personnel Qualifications
  - Past Performance
- ESS IA Approach
- Summary



# IA Overview



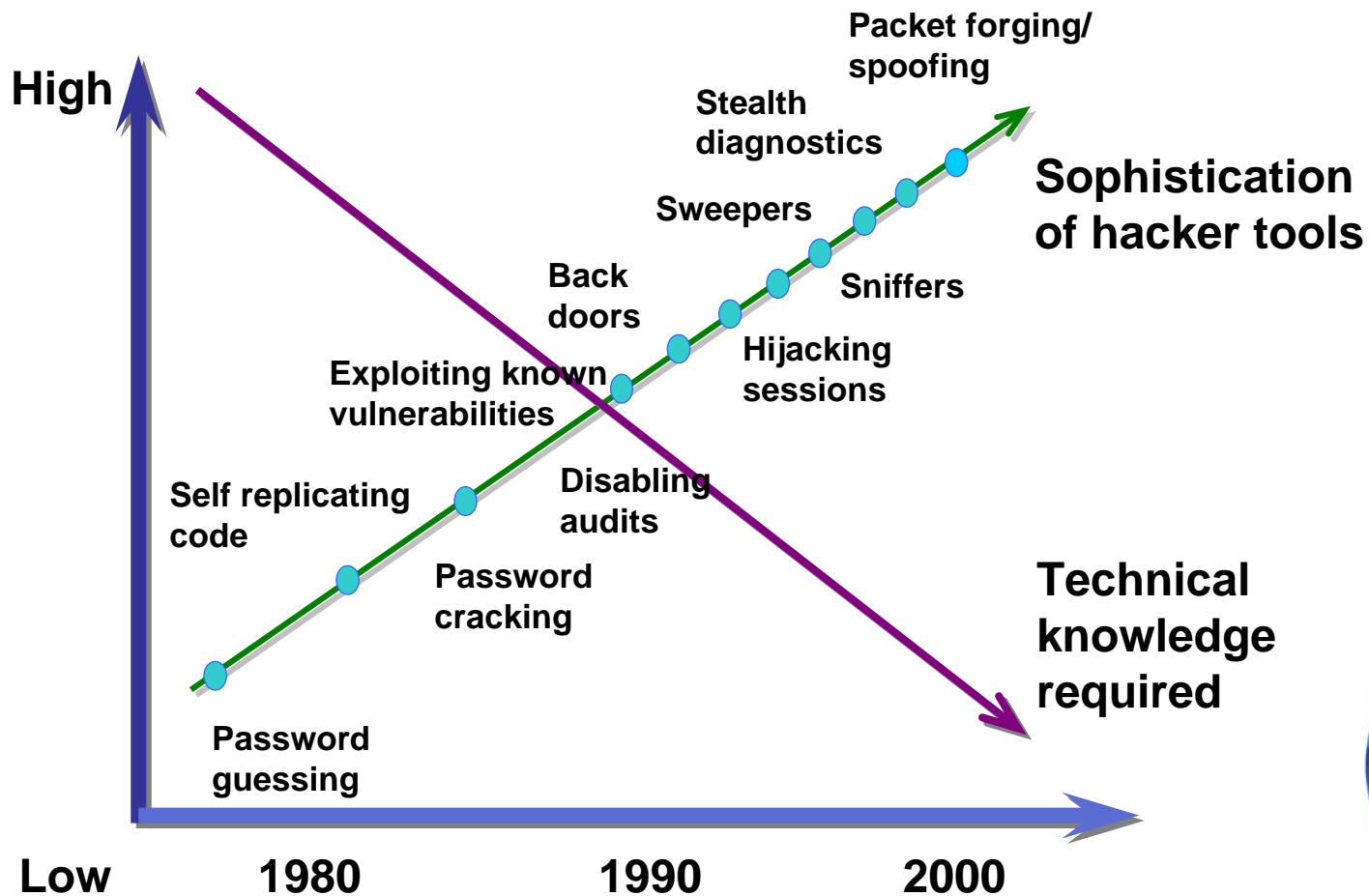
## What is Information Assurance?

The technical and managerial measures designed to ensure the confidentiality, integrity, authenticity, and availability of information and information systems. This includes the protection of data and devices against unauthorized access, use, disclosure, disruption, modification, or destruction. Information assurance also incorporates protection, detection and reaction capabilities for restoration of information and information systems. This term, which has spread from government use into common parlance, is sometimes synonymous with information security; however, IA covers a much broader perspective which involves a good deal more than just information security.



# Evolution of Threats Over Time

Hacker tools are becoming easier to use and more sophisticated



# Related Costs of Security Incidents are Rising



The costs associated with incident response and recovery have been extensive for many global organizations. Some examples are:

- A data heist at TJX is estimated to have cost the company a total of \$139 million
- BJ Wholesalers experienced a compromise that may have exposed the credit card information for an undisclosed portion of its 8 million members
- OfficeMax is the at the heart of a major data-security breach affecting as many as 200,000 consumers



# Government Drivers

-Include, but are not limited to:

- Clinger-Cohen Act
- Federal Information Security Management Act (FISMA)
- The Privacy Act of 1974
- DIACAP
- DCID 6/3
- DHS 4300
- ICD 503 (Non-concurred)
- NIST 800-series guidelines
- NIST SCAP



# Government and Industry IA Challenges



- Potential impacts to program funding
- Understanding new laws, directives, and guidance
- Change management and other organizational processes not followed consistently
- Need for clearly defined roles, responsibilities and separation of duties
- IA not addressed early on in system development life cycle (SDLC)
- Growing requirements due to increasing network complexity and interconnectivity
- Difficulty in hiring and retaining qualified IA professionals



# ESS IA Capabilities



## Security Reviews and Audits

An in-depth review will be conducted of all aspects of the organization to identify the threats, vulnerabilities and risks and to develop mitigation strategies.

## Certification and Accreditation

Experience with the entire certification and accreditation process in compliance with standards.

## Penetration Testing

The testing process involves an exploration of the all security features of the system in question, followed by an attempt to breach security and penetrate the system.

## Vulnerability Assessments

Assessments of system risks, and prioritization of their criticality, are performed based on accurate and timely threat analysis.



# ESS IA Capabilities (cont'd)



## Privacy Impact Assessments

PIA, as required by the E-Government Act, is an assessment of actual or potential impacts which a system may have on privacy.

## Security Event Auditing and Analysis

Auditing the security event logs for an organization can provide details about both outsider attacks as well as the abuse of rights by an insider.

## Incident Monitoring, Reporting and Recovery

Incidents can be accidental incursions or deliberate attempts to break into systems and can be benign to malicious in purpose or consequence.

## Network Security Architecture and Design

Integrating your security plan into your enterprise as you design the infrastructure.



# ESS IA Capabilities (cont'd)



## Development of Security Policy & Procedures

Security measures audited and confirmed by a third party provide both the presence of mind and confidence needed to ensure your data is protected and your policies are executed.

## Disaster Recovery & Continuity Planning

Disaster recovery and business continuity planning are processes that help organizations prepare for possible disruptive events

## Security Risk Management

Balance between compliance and risk management ...enables managers and technicians to better understand their system security posture.



# ESS IA Capabilities (cont'd)



## Security Awareness and Training

Providing a robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities.

## Intrusion Detection and Intrusion Prevention Systems

We offer proactive protection with an Intrusion Detection solution that fits your enterprise and your budget.



# ESS IA Personnel Qualifications



The Information Assurance and Network Security Division consists of a cadre of highly skilled IA professionals who:

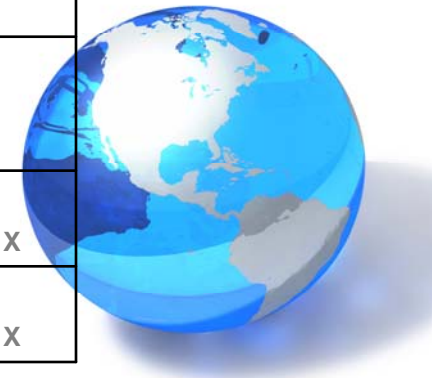
- Hold Top Secret clearances and possess both Counter-Intelligence and Full Scope Polygraphs
- Are CISSP and CAP certified
- Possess a multitude of industry-respected credentials to include MSCE, CEH, GIAC, Security+, as well as Oracle, Sun and ArcSight certifications
- Provide extensive potential for reach back and staff augmentation



# Past Performance



Customer / Functional Area	Certification and Accreditation	Security Risk Management	Intrusion Detection and Intrusion Prevention	Enforced Policies & Procedures	Network Security Architecture and Design	Vulnerability Assessments
U.S. Air Force Office of Special Investigations	X	X	X	X	X	X
Intelligence Community	X	X	X	X	X	X
U.S. Army	X	X		X	X	X
Department of Homeland Security	X	X	X	X		X
U.S. Navy Cyber Defense Operations Command (NCDOC)	X	X	X	X		
U.S. Navy Information Operations Commands (NIOCs)	X	X		X		
National Reconnaissance Office (NRO)	X	X	X	X	X	X
National Security Agency (NSA)	X	X	X	X	X	X





# Past Performance (cont'd)

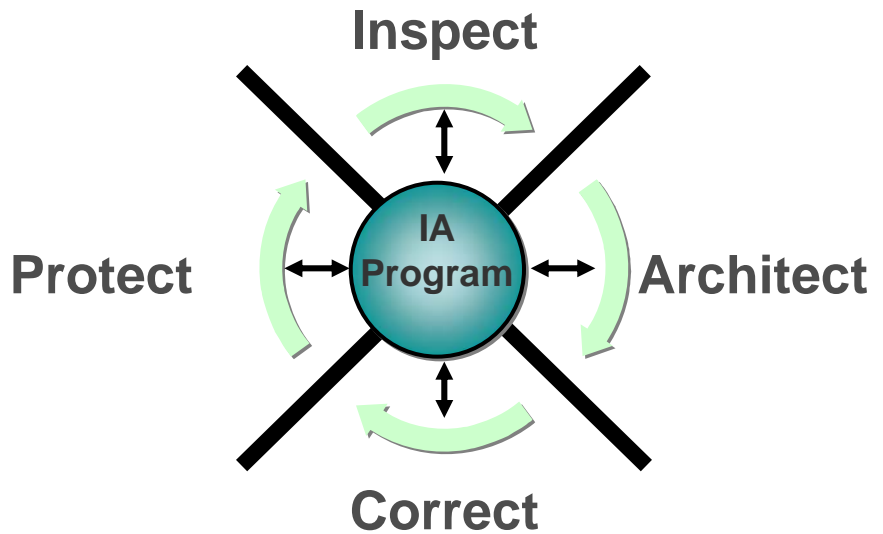
Customer / Functional Area	Certification and Accreditation	Security Risk Management	Intrusion Detection and Intrusion Prevention	Developed Policies & Procedures	Network Security Architecture and Design	Vulnerability Assessment
National Biodefense Analysis and Countermeasures Center (NBACC)	X	X	X	X	X	X
Battelle National Biodefense Institute (BNBI)	X	X	X	X	X	X
AT&T	X	X	X	X	X	X
Defense Information Systems Agency (DISA)		X	X	X	X	
US Air Force Space Systems		X		X		X
US Army SAP Community – Technology Application Office (TAO)	X	X		X	X	X
US Navy IT Telecommunications						
Office of the Director of National Intelligence (DNI)	X	X		X		X
Lockheed Martin						
General Dynamics		X		X		X
SAS® Institute, Inc.		X	X		X	X



# ESS IA Approach

The ESS IA Approach is divided into four phases to emulate phases of the System Development Life Cycle (SDLC):

- Inspect
- Architect
- Correct
- Protect

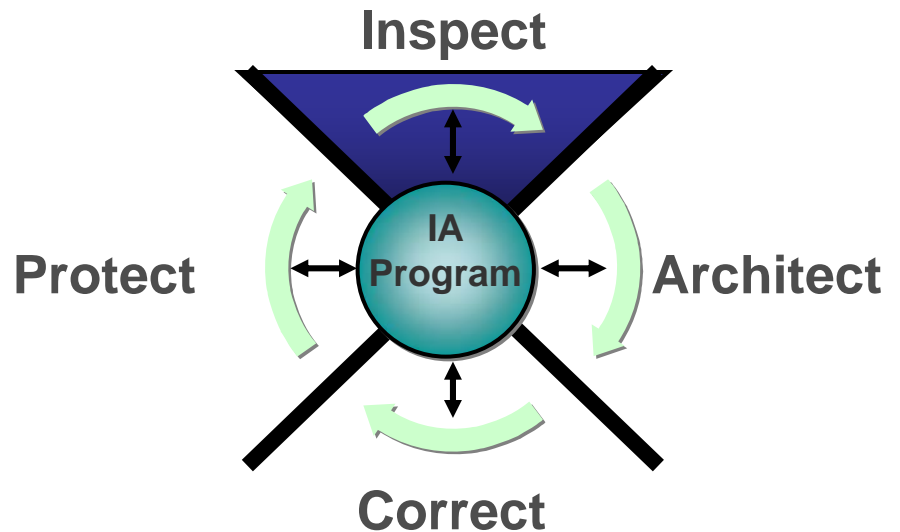


# ESS IA Approach **Inspect**



The Inspect Phase of the IA Approach deals with inspecting the current environment and planning the changes that need to take place. Some of the steps that occur during this phase include:

- Identifying IA requirements
- Conducting interviews to determine the state of the organization's security posture
- Determining security controls needed by conducting a threat and risk assessment
- Planning IA budget for IA life cycle

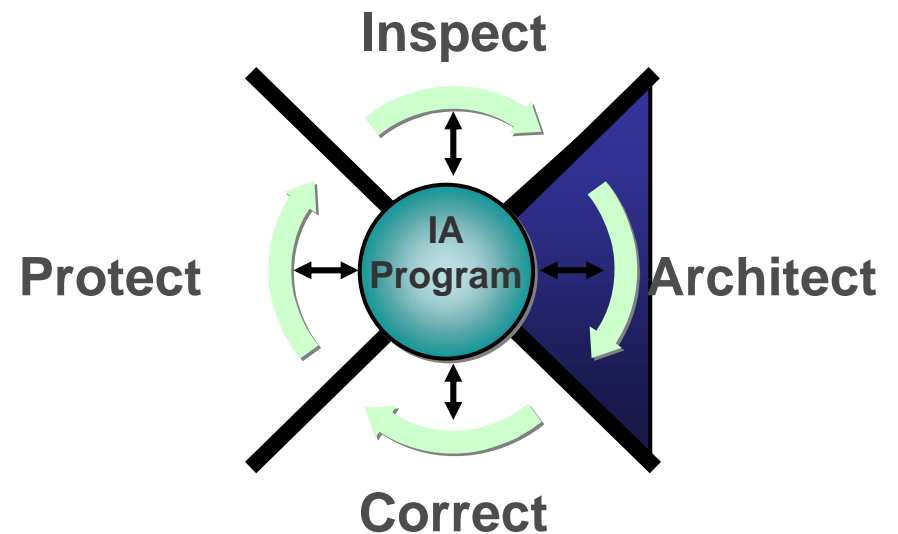


# ESS IA Approach Architect



This phase of the IA Approach involves architecting a solution based off of the information gathered during the Inspection phase.

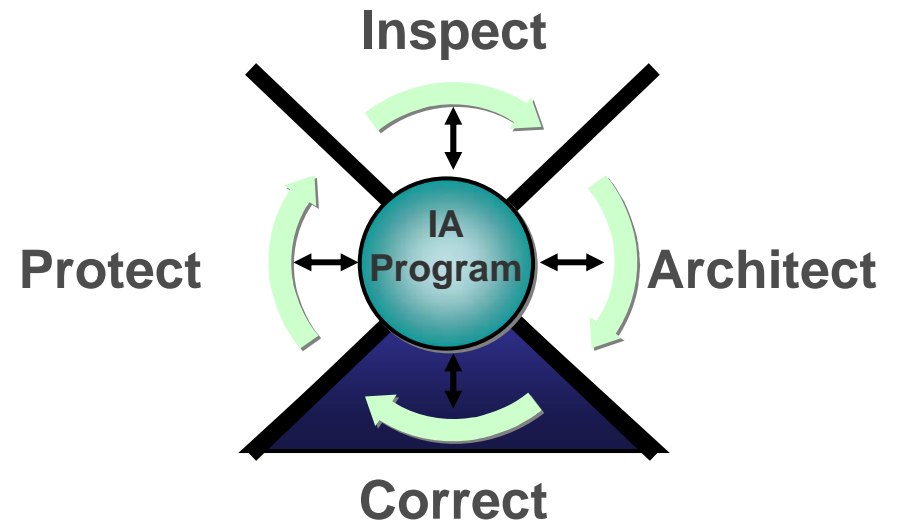
- Technology and system development
- IA product selection
- Generation of documentation to include plans, policies, procedures, accreditation packages, etc.



# ESS IA Approach **Correct**

The Correct Phase of the IA Approach is where the plans and controls developed during the first two phases are implemented and therefore “correct” the state of the organization’s security posture

- Incorporate IA strategies in System Engineering
- Procure and implement IA enabled products
- Conduct user awareness training
- Test and evaluate IA solutions
- Accredite information systems

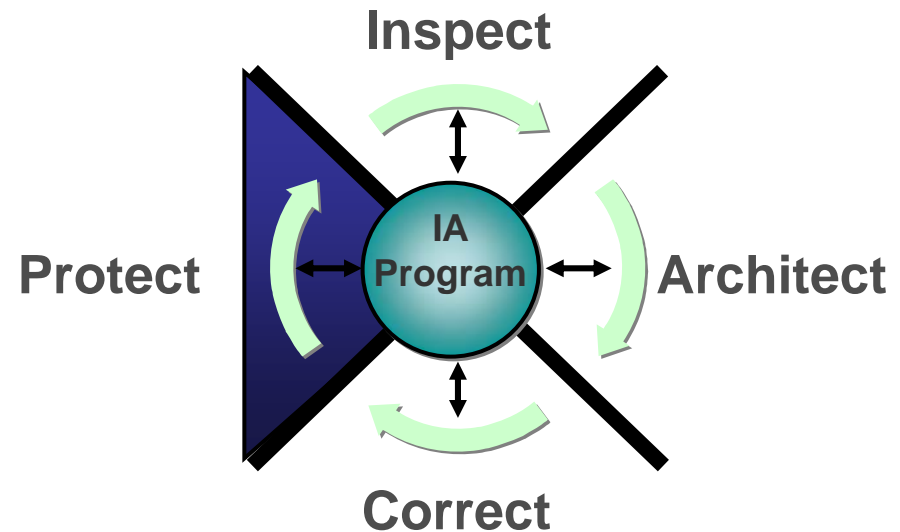


# ESS IA Approach **Protect**



The Protect Phase of the IA Approach is where continuing maintenance of the IA program occurs. This phase includes:

- Maintaining the system security posture throughout the life cycle by performing threat and risk assessments of the enterprise
- Assessing IA solutions to ensure that requirements are still being met and have not changed as the system matures
- Conducting re-accreditation tasks as required



# Summary



ESS has extensive experience in all aspects of the Information Assurance arena and can offer many value added IA and IT solutions to both our customers and our business partners.



# Contact Information



For additional information on our IA Support and Services please email ESS at [information@essworld.net](mailto:information@essworld.net) or call toll free at 1-800-854-1178

