ArcGIS in a Cybersecurity Environment

GIS in Defense and Intelligence

Ronald Moore and Robert “Glenn” Carr
Agenda

- Presentation Abstract and Presentation Objectives
- Our Modeling and Simulation (M&S) Program
  - What we do with geospatial data, and how we use ArcGIS
- Esri ArcGIS in Our M&S Program
  - What we use of the Esri products and tools
- Our M&S Program in our Cybersecurity controlled Computing Environment (CE)
  - An introduction to Risk Management Framework (RMF)
- Esri ArcGIS in our Cybersecurity controlled CE
  - Our ArcGIS Cybersecurity experience
- Our Final Products
- Questions
Presentation Abstract

- This paper presents the processes and tools, successes and challenges in the installation and maintenance of ArcGIS in a U.S. DoD Risk Management Framework (RMF) cybersecurity-enabled computing environment (CE). RMF provides security controls within the enterprise CE and a framework to assess the security posture of the CE. These controls provide guidelines that can be used by all ArcGIS users to ensure their systems and data are protected from malicious activities, even if RMF is not required.
Presentation Objectives

- Share our experience using ArcGIS in a Cybersecurity controlled Computing Environment (CE)
  - SE Core is a large U.S. Department of Defense contract
  - National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) Cybersecurity accreditation is required
- Looking for others with similar geospatial challenges
  - Desire to leverage other experiences
  - Potential collaboration
- Offer to share what we have done
  - All of our program products are available to U.S. DoD programs
  - Potential collaboration
Our Modeling and Simulation (M&S) Program

ArcGIS in a Cybersecurity Environment
Mission: Provide common correlated terrain databases, common models, standard simulation components, and common simulated forces to enable meaningful interoperability and facilitate fair fight in simulators and simulations.
Collect and process geospatial source data to create runtime terrain databases for mission training systems.
**Geospatial Terrain Generation Process**

- **Terrain Database Content Requirements**
- Source Data Collection, Standardization, and Conflation
- Vector Data Processing
- 3D Model Generation
- Airfield Vector Creation
- **Master Terrain Database Population**
- Map Generation
- Dataset Specialization
- Runtime Terrain Database Generation
- Runtime Terrain Database Integration & Test
- **Product Delivery**
Geospatial Terrain Generation Process

- Terrain Database Content Requirements
- Source Data Collection, Standardization, and Conflation
- Vector Data Processing
- 3D Model Generation
- Airfield Vector Creation
- Master Terrain Database Population
- Map Generation
- Dataset Specialization
- Runtime Terrain Database Generation
- Product Delivery

ArcGIS is used in six of our eight major processing steps

Deferred model creation
Source Data Collection, Standardization, and Conflation

Over 100 approved sources

Translate data model and dictionary; project to coordinate system

Conflation feature geometry and attributes to single source

Obtain (ship or download) source data for training location

Raw Source Data

Single Source Data

Translate

FACC  
NFDD  
EDCS
Vector Data Processing

Vector Editing includes cleaning, aligning and digitizing features to match reference aerial imagery.

Correct

Incorrect

Areal Alignment

Linear Alignment

Point Alignment

Our ArcGIS plugins provide error detection, reporting, and some automated correction of feature data.

Using Spatial Analyst 3D Analyst

Vector Data Processing

Requirements Source Collection Vector Data Processing Populate Master Database Dataset Specialization Map Generation Runtime Database Generation 3D Model Generation Airport Vector Creation Integration & Test Delivery
Airfield Vector Creation (1/2)

We enhance raw source data with airport specific information

Raw Source
Airfield Vector Creation (2/2)

Includes runway and taxiway lights and 3D model signage placement
Master Terrain Database (MDB) Population

The Master Database is the SE Core program’s data repository of all cleaned source data, simulation intensified source data, and specialized for customer (confederate) source data – using folder, files, and Esri SDE and FileGeoDatabase.
Map Generation

Using Defense Mapping and Production Mapping

Produce Topographic Line Map (TLM) 1:50K scale and 1:100K and Joint Operations Graphic (JOG) 1:250K scale

Distributed in GeoTIFF, JPEG2000 and CADRG formats
Dataset Specialization (1/2)

Scatter and Intensification

Automatically populate building footprints in areas missing extracted buildings

Missing Buildings

Synthetic Imagery

Create correlated aerial imagery from feature data

Color Map

Material Map

Adding simulation specific information

Requirements

Source
Collection
Vector Data Processing
Populate Master Database
Dataset Specialization
Map Generation
Runtime Database Generation
3D Model Generation
Airport Vector Creation
Integration & Test
Delivery

Synthetic Imagery

Scatter and Intensification
Dataset Specialization (2/2)

**Automated Modelization**

From feature footprint, height, roof type, and building function procedurally generate 3D models with interiors.

**Footprint**

**Tunnel Creation**

Generate tunnels from linear features and 3D model with couplers.

Subway station and tunnels.
Delivered terrain databases for active shooter response training

Hospital

Elementary School
Terrain Databases Produced for Training Systems (2/4)

Delivered terrain databases for military operation in urban terrain training

Enterable Building

Walls and Compounds
Delivered terrain databases for natural disaster response training

Cockpit View of UH-60L/M Flight Simulator

Required Multi-state models

Undamaged

Damaged

Cleared

Required Street Addresses

EURONAV®

Cleaned Marking Required
Delivered terrain databases for maneuver, collective, gunnery and artillery training
Esri ArcGIS in Our M&S Program

ArcGIS in a Cybersecurity Environment
SE Core Esri ArcGIS Products

- **ArcGIS Desktops**
  - (~75) ArcGIS Desktop Advanced
  - (~20) ArcGIS Spatial Analyst for Desktop
  - (~20) ArcGIS 3D Analyst for Desktop
  - (~15) ArcGIS Defense Mapping Concurrent
  - (~75) ArcGIS Pro

- **ArcGIS Servers**
  - (2) ArcGIS for Server Enterprise Advanced
    - Image Extension for Server Enterprise Advanced
    - Esri Defense Mapping for Server Enterprise Advanced
    - Esri Production Mapping for Server Enterprise Advanced
    - Web Adapter
  - (1) ArcGIS License Manager
Major ArcGIS Plugin Developer

- Over 70,000 lines of code in our ArcGIS Utilities
  - 60% C#
  - 30% C++
  - 10% Python

- Over 200 specific ArcGIS add-on tools, for example
  - EDM Translations tools
  - Attributes cleanup tools
  - Content and quality geometry check and correct tools
  - Content and quality attributes check and correct tools
  - Map production automation tools
  - Quality Control (QC) tools
  - SDE Create, Merge and Split tools
  - Layer and delayering tools
  - Conflation tools
XML To Points
Video Browser
Vector Field Populator Tool
VCDR: Find Dangling Lines
VCDR: Z Fighting Intersections
VCDR: Vert Count Report
VCDR: Unique Attributes Report
VCDR: Unclosed Areal Features
VCDR: T-Vertex Fixer
VCDR: Trim All String Attributes
VCDR: Too Small Between Intersections
VCDR: Too Many Vertices
VCDR: Too Close to Intersection
VCDR: Switchback Roads
VCDR: Skeepe Bridge
VCDR: STAT Topology Errors Report
VCDR: Snapping
VCDR: Simplicity Geometry
VCDR: Shrink Overlapping Hydro Buffers
VCDR: Sharp Angles Between Lines and Areal
VCDR: Sharp Angles Between Lines
VCDR: Self Intersecting
VCDR: Scale JOG Sheets North and East
VCDR: Sawtooth Bridge
VCDR: Road Vertices in Hydro
VCDR: Road Processor for Maps
VCDR: Road Ending In Hydro
VCDR: Road Above Minimum Elevation
VCDR: Road & Rail Merger
VCDR: Reports Vertices Too Close
VCDR: Report Powerline Overlaps
VCDR: Report Close Neighboring Points
VCDR: Report Bad Lane Changes
VCDR: Report Attributes with Bad Characters
VCDR: Remove Unclosed Areal Features
VCDR: Remove Point Peaks from Hydro
VCDR: Remove Null Geometry
VCDR: Remove Neighboring Vertices Within Tolerance
VCDR: Remove Near Duplicates
VCDR: Remove Features With Duplicate Geometry
VCDR: Remove Collinear Vertices
VCDR: Remove Close Vertices
VCDR: Remove Areal Contains Areal
VCDR: Rdgt_thinning Field Value Report
VCDR: Problem Ramp Finder
VCDR: Populate building_interior Field
VCDR: Populate bridge_over_water Field
VCDR: Overlapping
VCDR: Nullify Empty Strings
VCDR: Null Geometry Report
VCDR: Non Trimmed Strings Report
VCDR: Non Simple Geometry Report
VCDR: Near Duplicates
VCDR: Multipart Report
VCDR: Layer Level Validator
VCDR: JOG Sheet Purlifier
VCDR: Isolated Geometry Report
VCDR: Generate Label From Feature Class Name
VCDR: Fix Labels With Bad Characters
VCDR: Fix Attributes With Bad Characters
VCDR: Find Overlaps Across Areal
VCDR: Find Incorrectly Split Transportaion
VCDR: Find Gaps Across Areal
VCDR: Find Crossing Lines
VCDR: Find Areal Within Areal
VCDR: Filter Bulleye Contours
VCDR: Features Without Label Report
VCDR: Features with Zs Report
VCDR: Features with Slivers
VCDR: Features with Duplicate Geometry Report
VCDR: Features with Duplicate Geometry and Attributes Report
VCDR: Features with Bad Width Report
VCDR: Features with Bad Characters Report
VCDR: Feature Validator
VCDR: Feature Count
VCDR: Extend Line
VCDR: ESRI Check Geometry Report
VCDR: Empty Strings Report
VCDR: EDM Validator
VCDR: Cut Areal Holes
VCDR: Count Areal Holes
VCDR: Convert Accidental Nulls to Real Nulls
VCDR: Clear all rdgt_thinning fields
VCDR: Clean Z Values
VCDR: Bridge Vertices
VCDR: Bridge Tunnel Lane Intersection
VCDR: Bridge Road Elbow Junctions
VCDR: Bridge Intersection
VCDR: Bridge Clearance
VCDR: Attribute Case Fixer
VCDR: Add Runway Attributes to Point Aerodrome
VCDR: Accidental Nulls Report
VCDR: EDM Validator
VCDR: EDM Translation
VCDR: EDM Ruleset Editor
VCDR: EDM Processing
VCDR: Edit Session Tracker
VCDR: Duplicate Anno Remover
VCDR: Drop Empty Feature Classes
VCDR: DEM Processor
VCDR: Database Splitter
VCDR: Conflation
VCDR: Confederate Differentiation Tool
VCDR: CEDG Batch Reproject
VCDR: By Name Loader
VCDR: Building Footprint Adjustment
VCDR: Buffer Linear
VCDR: BUA Power Line
VCDR: BUA Buildings (areal)
VCDR: BUA Buildings
VCDR: Browse Features
VCDR: Batch Geotiff Export
VCDR: Batch Annotation Merge
VCDR: Auto Snapper
VCDR: Auto Redraw Tools
VCDR: Attribute Wizard
VCDR: Attribute Field Populator Tool
VCDR: ArcGIS Spatial Analyst
VCDR: ArcGIS Server
VCDR: ArcGIS Image Server
VCDR: ArcGIS Desktop
VCDR: ArcGIS Data Reviewer
VCDR: ArcGIS 3D Analyst
VCDR: Arc Catalog
VCDR: AOI Calculator
VCDR: Airport Wizard FLT to GDB
VCDR: Maps Aggregator
VCDR: ADIZ to GOLDEN
VCDR: ADI Identifier
VCDR: Add Point Peak Elev Fields

SE Core ArcGIS Plugin Tools

©2017 LEIDOS. ALL RIGHTS RESERVED.
Our M&S Program in our Cybersecurity controlled Computing Environment (CE)

ArcGIS in a Cybersecurity Environment
Why do we need Cybersecurity?

- For our program it is a requirement of our contract
- Regardless of contractual requirements, adequate cybersecurity:
  - Protects data (geospatial)
    - Data may contain sensitive information
    - Integrity of data is crucial
  - Protects the investment
    - Value of hours spent creating data
    - Potential schedule risk if data lost
  - Protects the equipment
    - Maintain positive control of computer assets
    - Liability if equipment is utilized for cyber attack
  - Protects the users
    - User and account name
    - Contact information
What is a Security Framework?

- A series of documented processes that are used to create policies and procedures around the implementation and ongoing management of information security controls in an enterprise computing environment
  - Guides the implementation
  - Manages the security controls

- A "blueprint" for building an information security program to manage risk and reduce vulnerabilities

- Numerous Frameworks available
  - ISO / IEC 27001 (International Standard)
  - OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  - NIST Cybersecurity Framework (CSF)
  - NIST Risk Management Framework (RMF) (DoD required)
National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)

- Select security controls; applied tailoring guidance and controls based on risk assessment (FIPS 200/SP 800-53)
- Implement security controls using engineering practices; applied security configuration settings (FIPS SP 800-70)
- Defined network critical/sensitive according to worst-case adverse impact to mission (FIPS 199/SP 800-60)

Continuous monitor and track changes that affect security controls, execute life cycle (FIPS SP 800-37/SP 800-53A)

Authoring Official (AO), determine risk; authorize operation (FIPS SP 800-37)

U.S. Army Information Systems Engineering Command (USAISEC) reviewed and determined security controls effectiveness (FIPS SP 800-53A)

NIST Special Publication 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems"
Resources

- To use eMASS, you must have access to a .mil network segment. It is not reachable by commercial internet
Esri ArcGIS in our Cybersecurity controlled CE

ArcGIS in a Cybersecurity Environment
Implement Cybersecurity - Network, Servers, Workstations and Applications (1/2)

- Overarching – Application of tested security updates within DoD Information Assurance Vulnerability Management (IAVM) published timelines, continuous monitoring of audit logs from all systems, reoccurring system wide discovery and vulnerability scans, implement access controls to restrict user access to only approved areas

- Network – [Network Switches and Routers, Firewall] Access control restricted, only approved protocols enabled, all ports, protocols, and services are documented and registered, encryption algorithm restricted to FIPS 140-2

- Servers – Disabled unproved and unused services, no elevated user access, Host Based Security System (HBSS) deployed with virus protection, file integrity monitoring, on-access scan, Host intrusion Prevention System (HIPS), Public Key Infrastructure with token based logon, and firewall deployment
Implement Cybersecurity - Network, Servers, Workstations and Applications (2/2)

- Workstation – Disabled unproved and unused services, limited elevated user access, Host Based Security System (HBSS) deployed with virus protection, file integrity monitoring, on-access scan, Host intrusion Prevention System (HIPS), Public Key Infrastructure with token based logon, and firewall deployment

- Applications – Restricted to Commercial (COTS) and Government (GOTS) products that are vulnerability scanned and Configuration Control Board (CCB) approved, internally develop products that comply with development standards, Open Source products that are treated with the same level of scrutiny as internally developed tools, apply all applicable DoD-provided security technical implementation guidelines (STIG)
Segmented Network Design

- Enclave Test & Development STIG requires segmented environment
- Both terrain generation and software development environments are required to be configured IAW DoD technical guidelines

Terrain Generation Network
- No administrative privilege
- Internet access restricted to approved sites to support source data exploitation
- Security configuration is tightly managed as focus for this environment is on controlled repeatable processes
- Compliant with DoD Security Requirements

Software Development Network
- Administrative privileges required
- Internet access restricted - blocked software downloads
- Security configuration changes for development network serve as a test and validation of configurations before they are applied to the terrain generation network
- Security settings can be adjusted in a controlled manner to facilitate testing as needed
Additional Development Network Requirements

- Additional requirements for Development Environment and Activities
- Adhere to industry recognized coding standards
  - Documented development standards and coding guidelines
  - Enforced through code peer review
- Requires use of approved automated Static Code Analyzer (SCA)
  - HP Fortify
- Requiring FIPS 140-2 compliant encryption algorithms
  - Broke some internally developed tools
  - Required code correction to resolve
- Open Source Tools / Products are required to go through the same scrutiny as internally developed products
  - Open Source Product source code must be run through SCA
  - Any identified insecure coding practices must be corrected
Our SE Core ArcGIS Computing Environment

Our ArcGIS deployment segmented into Terrain Generation and Development networks, with daily backup and internet access.
Our SE Core ArcGIS Computing Environment

- ArcGIS deployment is also segmented between Terrain Generation and Software Development
- SQL servers and ArcGIS servers required on separate physical hardware per SQL STIG
- Development cannot use ArcGIS Online Community Resources
  - Controlled distribution of SE Core data products prohibits sharing our tools and data products to the public
  - Cannot download or use plugins that haven’t gone through our required extensive review and approval process
    - Code analysis required
    - Secure coding practice must be ensured
- Esri ArcGIS Server has applied DoD approved STIG
- Esri ArcGIS for desktop currently does not have a STIG
**ArcGIS for Server 10.3 Security Technical Implementation Guideline**

- Developed by Esri and DISA for the DoD and published 2/26/16
- Configured on both Software Development and Terrain Generation ArcGIS implementations
- Consists of multiple configurations that are audited with 22 checks

<table>
<thead>
<tr>
<th>IIS - 5 checks</th>
<th>ArcGIS Srvr - 14 checks</th>
<th>OS – 4 checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SSL requirement</td>
<td>• HTTPS only</td>
<td>• Audit file and directory permissions</td>
</tr>
<tr>
<td>• Windows Authentication enabled</td>
<td>• Authentication Tier = Web Tier</td>
<td>• FIPS algorithms</td>
</tr>
<tr>
<td>• Anonymous Connection disabled</td>
<td>• Log levels = Verbose</td>
<td>• Encryption (if required)</td>
</tr>
<tr>
<td>• Client certs required</td>
<td>• Update *.json files to have isolation level of HIGH</td>
<td>• All other applicable STIGS to the OS</td>
</tr>
<tr>
<td>(CAC login)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©2017 LEIDOS. ALL RIGHTS RESERVED.
RMF Implementation Impacts to ArcGIS

- **Security and Functionality**
  - Implementation of technical security controls related to RMF resulted in no failures of Esri Products in our facility.
  - SE Core plugins required update.

- **Security and Performance**
  - Implementing technical controls, as required by RMF, impacted user performance negatively, both directly and indirectly.
  - Direct Impact: McAfee Antivirus implementation
    - On-Access Scanning impacted data access speeds at workstations.
    - Established exceptions for identified file types and locations, and only these types and these locations.
  - Indirect Impact: Logging and Auditing
    - Logging at the network, servers, workstations and applications, to support auditing requirements, impacted user performance.
    - Tailored hardware configurations to compensate for increased logging burden.
Our Final Products

ArcGIS in a Cybersecurity Environment
Examples of Terrain Products (1/6)
Examples of Terrain Products (2/6)
Examples of Terrain Products (3/6)
Examples of Terrain Products (4/6)
Examples of Terrain Products (5/6)
Examples of Terrain Products (6/6)
Questions (and Answers)

ArcGIS in a Cybersecurity Environment