

# Evidentiary Integrity for Incident Response (EIR)



## Cyber Security Division 2012 Principal Investigators' Meeting

11 October 2012

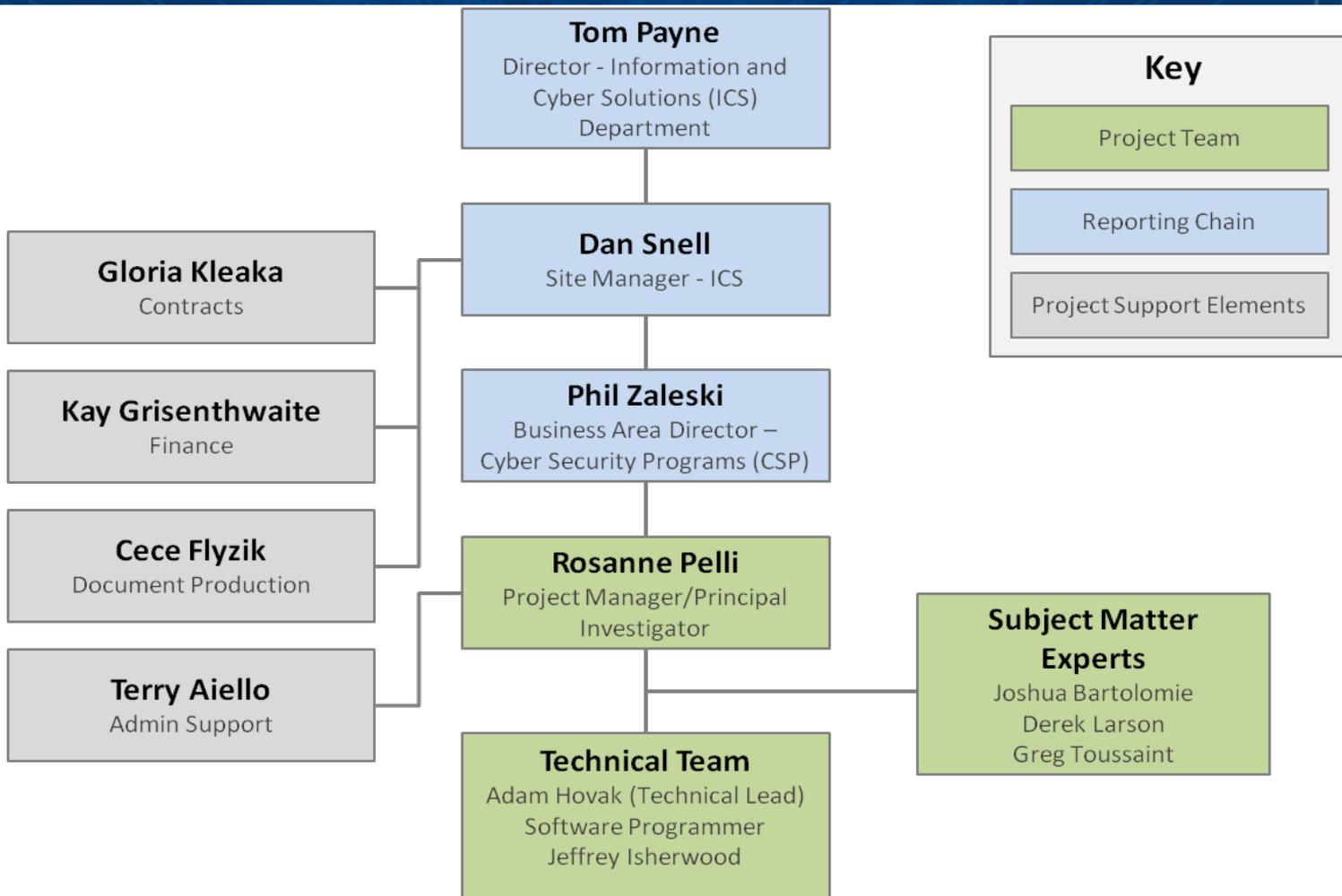
**Jeffrey Isherwood**  
**Senior Cyber Security Analyst**  
**Exelis Inc.**  
**Jeffrey.Isherwood@exelisinc.com**  
**315-838-7064**

# TTA #10: Digital Provenance

## Evidentiary Integrity for Incident Response (EIIR)

- Type I (New Technologies)
- Duration: 18 months
- Objective:
  - Improve the ability for non-forensic Incident Responders (IR) staff to perform local investigations that more adequately fulfill multiple legal, regulatory, or standards compliance requirements and best practices in relation to documentation, evidentiary handling, chain of custody, and integrity validation and non-repudiation.
  - Develop a seamless and customizable Windows® Operating System command shell interface/overlay called **Proactive Incident Response Command Shell (PIRCS)**

# The EIR Team

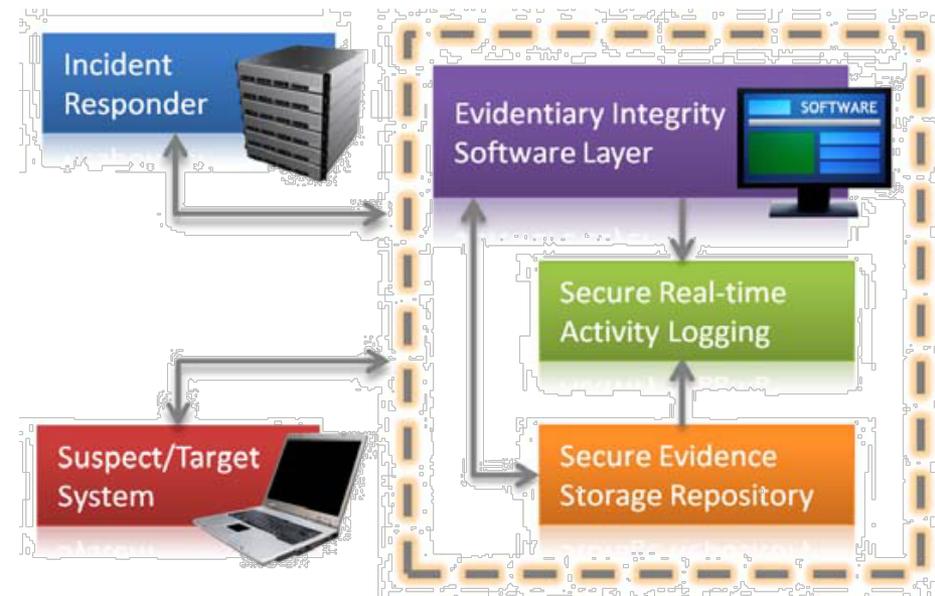


# Technical Approach

- **Current challenges to incident response evidentiary collection**
  - Compatibility, scalability, cost, remote installation and evidence collection
  - Communications and capabilities gap between LEO practices and IR teams
- **Technical Approach**
  - To analyze, design, prototype, develop, document, test and deliver the PIRCS capability to the Incident Responder community, to provide activity logging functionality as well as secure evidence collection during an investigation.
  - To leverage Incident Response and Cyber Forensic SMEs in the Exelis Cyber Incident Response Center(CIRC) to identify current gaps and requirements.
  - To develop PIRCS using an agile model, thereby allowing SMEs to provide feedback at various stages of development.

# Technical Approach (cont.)

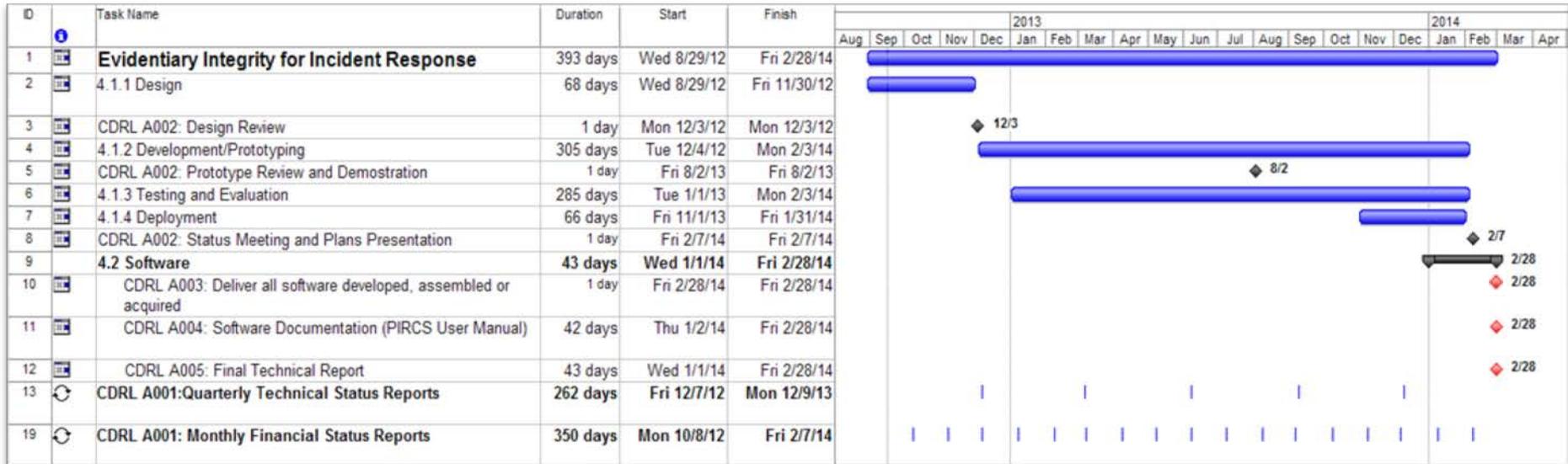
- **Design goals include**
  - Evidentiary source attribution
  - Evidence verification and validation
  - Evidence encapsulation & preservation
  - Customizable identity marking criteria
  - Multilayer object based identity markings
  - Non-reputable end-user activity and audit logging
  - Leverage the open-source “Advanced Forensic Format (AFF)” and define robust and secure encapsulation methods and metadata requirements



# Technical Approach (cont.)

- Modularize functional components to enable multi-scenario/industry customization and usage
- Automate evidentiary chain of custody documentation, security, and meta tagging
- Bind all actions to specific incident response actors and systems
- Prevent evidence and action repudiation
- Reduce incident response human error and/or documentation gaps
- Limit evidentiary mishandling, unauthorized access and/or unintended disclosure
- Increase incident response evidentiary viability and usability

# Schedule & Milestones



## Schedule & Milestones

- ◆ Design and validation: 3 months
- ◆ Development and stability testing: 12 months
- ◆ Prototype pilot, evaluation, and refinement: 3 months

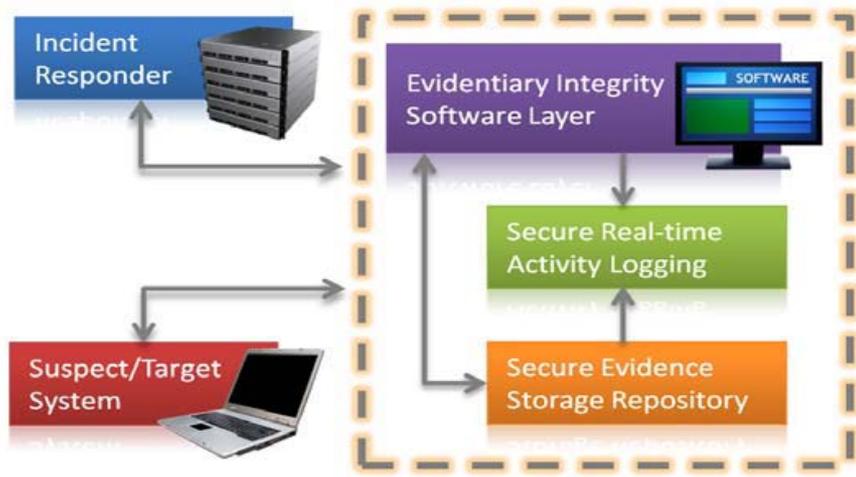
## Deliverables

- ◆ Monthly financial and technical status reports
- ◆ Prototype software
- ◆ Usage and administration guide(s)
- ◆ Final technical report

# Technology Transition Plan

- Pursue a transition and commercialization path for PIRCS and provide status updates on our progress. This plan includes:
  - Close interaction with the Incident Response and Cyber Forensic SMEs in the Exelis Cyber Incident Response Center(CIRC)
    - Perform operational test and validation of PIRCS throughout the entire development process
    - Create an initial transition path to an enterprise-level operations center
  - Leveraging Exelis' current commercialization channels to:
    - Offer PIRCS as a stand-alone product, utilizing our value added reseller channels
    - Or ...
    - Provide PIRCS, under license, to existing cyber forensic tool vendors for inclusion into their products
  - DHS CyberFETCH Information Sharing Web Portal
    - Within 120 days of the completion of the effort, if no clear commercialization paths have materialized - Exelis will release PIRCS source code to the public domain, most likely employing a Berkeley Software Distribution (BSD) license
    - Consumer: DHS cyber forensics and incident response communities

# Quad Chart



## Operational Capability

### Performance Targets:

- Address and mitigate specific investigatory shortcomings when utilizing the Windows Operating System Command Shell for Incident Response activities.
- Provide robust, standardized, automated, secure and non-refutable evidence artifact handling/tagging and chain of custody logging.
- Maintain evidentiary artifact(s) integrity during the execution of incident response or live forensics
- Minimize or reduce Incident Responders impact and overhead
- Provide usage customization options to maintain viability within multiple scenarios and industry requirements

## Proposed Technical Approach

Objective: Address TTA #10 with development of a software abstraction layer to be leveraged by incident and first responders that arbitrates interactivity and automatically initiates evidentiary logging, encapsulation, metadata population, and integrity validation processing.

Technical Approach: Leverage open-source “Advanced Forensic Format (AFF)” and define robust and secure encapsulation methods and metadata requirements

- Design a Windows OS based command shell interface that automates robust session logging, tagging, metadata population, and validation
- Modularize functional components to enable multi-scenario/industry customization and usage

## Schedule, Milestones & Deliverables

### Schedule and Milestones:

- Design and validation: 3 months
- Development and stability testing: 12 months
- Prototype pilot, evaluation, and refinement: 3 months

### Deliverables:

- Prototype software
- Final technical report
- Usage and administration guide(s)

# Questions?



[www.exelisinc.com](http://www.exelisinc.com)

# Thank You

## ITT EXELIS

**Rosanne Pelli**  
EIRR Program Manager

Information & Cyber Solutions  
474 Phoenix Drive  
Rome, NY 13441  
(315) 838-7068

[Rosanne.Pelli@exelisinc.com](mailto:Rosanne.Pelli@exelisinc.com)

PMP, CompTIA Security+

## ITT EXELIS

**Jeffrey Isherwood**  
Senior Cyber Security Analyst

Information & Cyber Solutions  
474 Phoenix Drive  
Rome, NY 13441  
(315) 838-7064

[Jeffrey.Isherwood@exelisinc.com](mailto:Jeffrey.Isherwood@exelisinc.com)

CISSP, CRISC, C|EH, Linux+, LIPC-1

## ITT EXELIS

**Phil Zaleski**  
Business Area Director  
Cyber Security Programs

Information & Cyber Solutions  
474 Phoenix Drive  
Rome, NY 13441  
(315) 838-7114

[Phil.Zaleski@exelisinc.com](mailto:Phil.Zaleski@exelisinc.com)

CISSP, CRISC