



Information Assurance and the Project Manager



Carmine F. Vilardi
Director, Mgm Operations
334-277-1972 Ext. 223
carmine.vilardi@engilitycorp.com

Why do we need address Information Assurance?

❖ IA is a significant part of information capability

In today's virtual world, most organizations operate across many different physical locations – such as:

* Customers * Industry Partners * Academia * Federal Agencies

It is necessary to depend upon large numbers of computer systems and networks and to manage them in an effective communications and information infrastructure

Unauthorized disclosure of information or compromise of computer systems could have a serious impact on business

— Government and business mandates are in place to proactively address these issues, and minimize risk for loss or compromise of data

So What Is the PM's Role?

❖ How then can the PM:

- Address system requirements?
- Maintain control on cost and schedule?
- Maintain or improve the IA posture of the project?
- Address or mitigate potential IA risks in operation?
- “Answer the mail” on mandates?



So What Is the PM's Role?

- ❖ **Excerpts from the Defense Acquisition Guidebook addressing Information Assurance.**
- ❖ The program manager should ensure that the Acquisition Strategy identifies the technical, schedule, cost, and funding issues associated with implementing information assurance.
- ❖ The planning for and documentation of the Acquisition IA Strategy should produce the information required.
- ❖ Potential IA considerations should be included in the Acquisition Strategy.
- ❖ The program manager should ensure the Acquisition IA approach compliments the corporate business and IT strategy.

Understand the Environment

- ❖ Is your companies' strategy moving toward network centricity? Service Oriented Architecture (SOA)?
- ❖ Do you have a Net-Centric Information Assurance (IA) Strategy?
- ❖ The intent of the Net-Centric IA Strategy is to reflect an approach to IA concepts and definitions from a "services" point-of-view instead of a "system" point-of-view, without specifying requirements related to specific implementations or architectures.
- ❖ Is there an end-to-end IA perspective?
- ❖ Is that perspective captured in a set of informational documents and/or architecture products (tools)

Information Assurance (IA) Center of Excellence (COE)

Information Assurance – “Measures that protect and defend information & information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. . . Include[s] providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.” (NSA glossary)
(CJCSI 3170.01C)

Center of Excellence – “Institution possessing special knowledge or expertise in a particular area. . . and incorporated into a collaborative environment to facilitate development of products supporting (key) functions and operations.” (USJFCOM glossary)



Highly skilled people using common processes, methodologies, & tools

Understand the Environment

- ❖ A Net-Centric information assurance construct:

- ❖ Conceptualized and specified for integration of IA into a net-centric information environment that is:
 - Secure
 - Globally interconnected
 - With an end-to-end set of information capabilities, associated processes, and personnel
 - Collecting, processing, storing, disseminating, and managing information
 - Providing it on demand users, policymakers, and support personnel.



❖ The program manager should:

- Incorporate information assurance requirements into program design activities

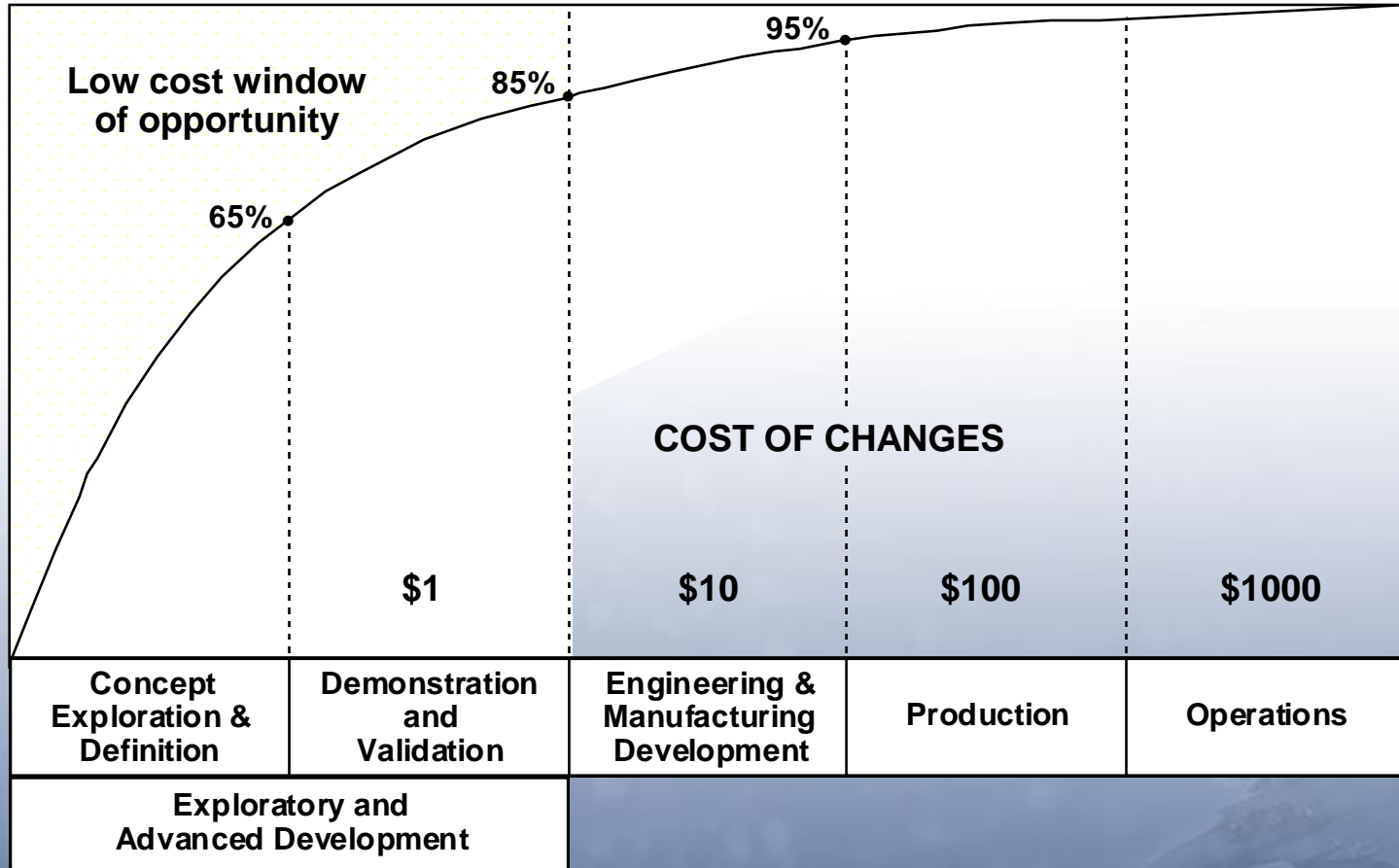
 - Ensure availability, integrity, authentication, confidentiality, and non-repudiation of critical system information.

- Examine his/her acquisition program carefully to identify applicable IA requirements.

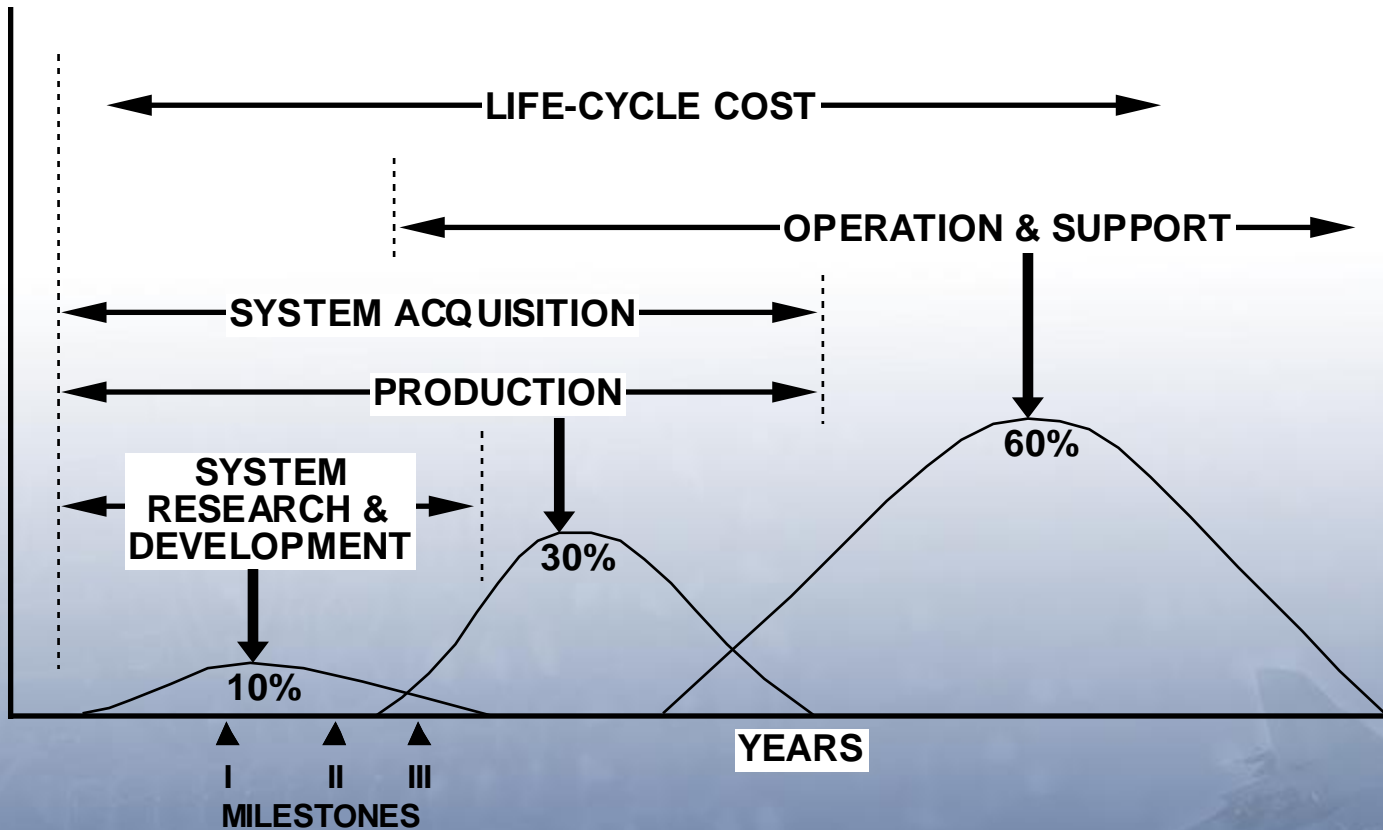
 - Since requirements for IA vary greatly across acquisition programs, it is essential that a program manager



85% Of 'Life Cycle Cost' is determined before System Development

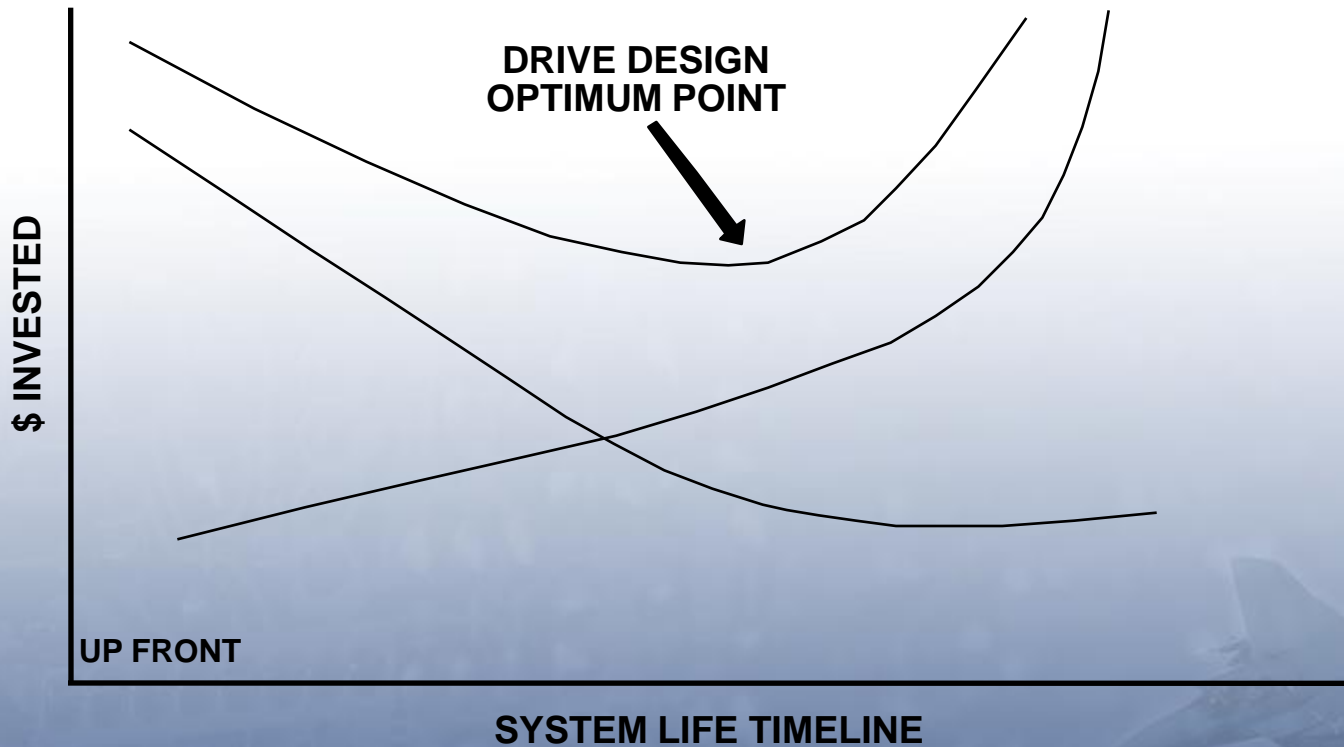


Typical System Life Cycle Cost Distribution



Optimizing Life Cycle Cost

LCC = ACQUISITION COST PLUS O&S COST



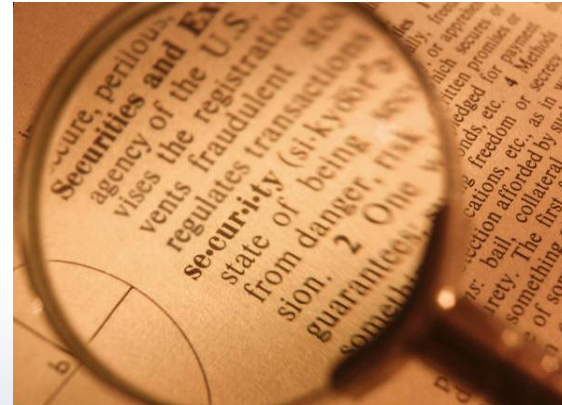
- ❖ Give system users/customers protection – flexibility
- ❖ Question the feasibility of the system in terms of data:
 - * Will it be protected? * Is it affordable?
 - * Will it be available? * Is it sustainable?
 - * Will it be trust worthy? * Will it be traceable?
 - * Will it be dependable?
- ❖ **Output**
 - Recommendations for system design for IA
 - System design artifacts
 - Test results and analyses
 - Potential risks and mitigation recommendations
 - Compliance with mandates
 - Better system protection at lower cost

❖ People tend to think “Security” when you say Information Assurance - it’s more

- Several disciplines and strategies coming together
- To ensure efforts progress with the most secure IS and data practical
- Placing a high priority on the IA elements:
 - Confidentiality
 - Integrity
 - Availability
 - Authentication
 - Non-Repudiation
- And provide for restoration of information systems by incorporating protection, detection, and reaction capabilities

Confidentiality

To make sure the information is protected from unauthorized disclosure.



Integrity

To ensure the information you use, transmit, process or store has not been corrupted or adversely manipulated.



Availability

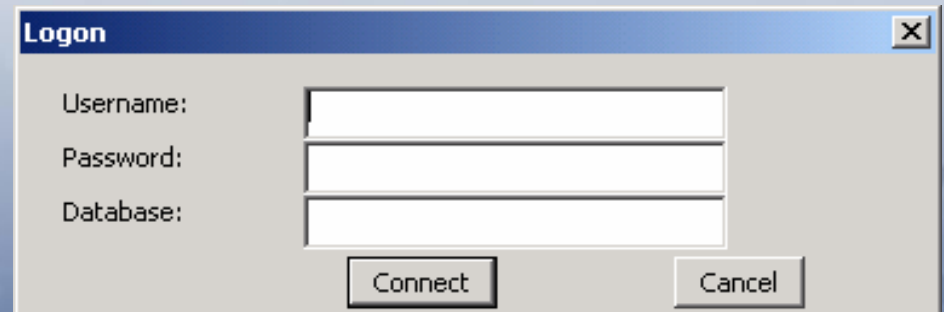
To make sure the computer and the information is there when we need it.



Authentication

To ensure that you have the right to see the information, and you are who you say you are by:

Verifying the identity of the user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.



A screenshot of a Windows-style dialog box titled "Logon". The dialog box has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains three text input fields stacked vertically. The first field is labeled "Username:", the second "Password:", and the third "Database:". Below the fields are two buttons: "Connect" on the left and "Cancel" on the right.

Non-Repudiation

To ensure the information is “tagged” resulting in the sender knowing it got there, and the recipient knowing who sent it.

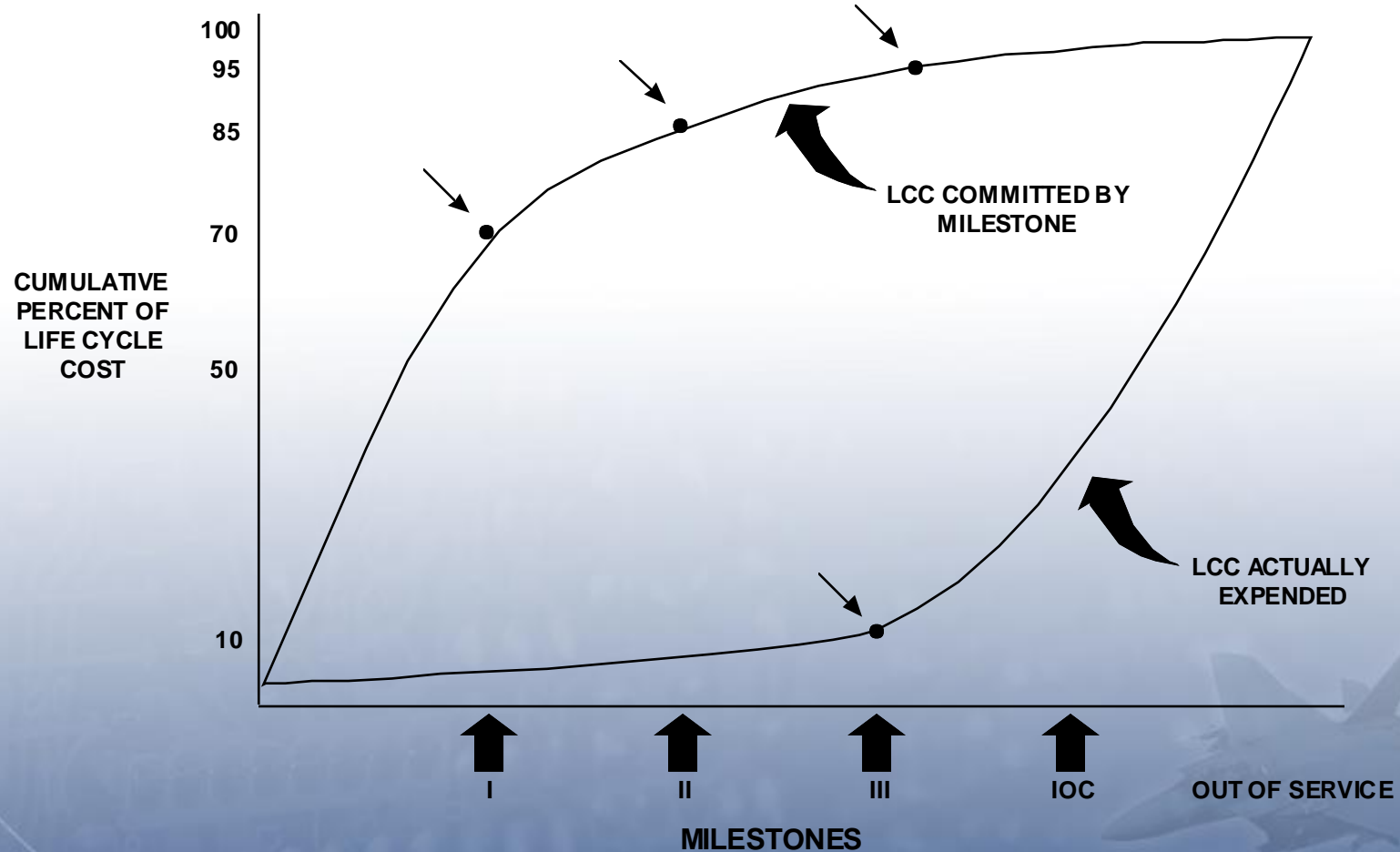
-in other words –

Assuring the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity - neither can later deny having processed the data.

- ❖ **Determine system IA requirements and characteristics**
 - In technologies & design
 - In the host system
 - In the enclave
 - In the enterprise

- ❖ **Study/analyze identified characteristics**
 - Make assessments of a particular technology or design in terms of IA considerations
 - Provide assessment results in terms of dependencies and risks
 - Document transition at a later time into system application
 - Develop system artifacts and “transition documents”

Typical System Life Cycle Cost Commitment vs Expenditure



- ❖ **Range of analysis**
 - How to analyze
 - What to analyze

- ❖ **Ask the right questions of the right people**

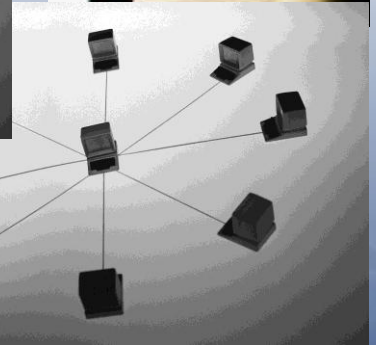
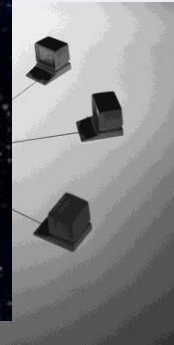
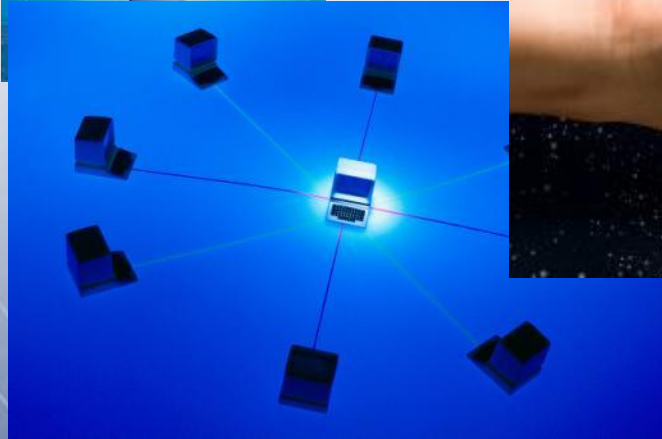
- ❖ **Know where to look for questions and resources (people/databases)**

- ❖ **Learn fundamentals/impacts of IA considerations**

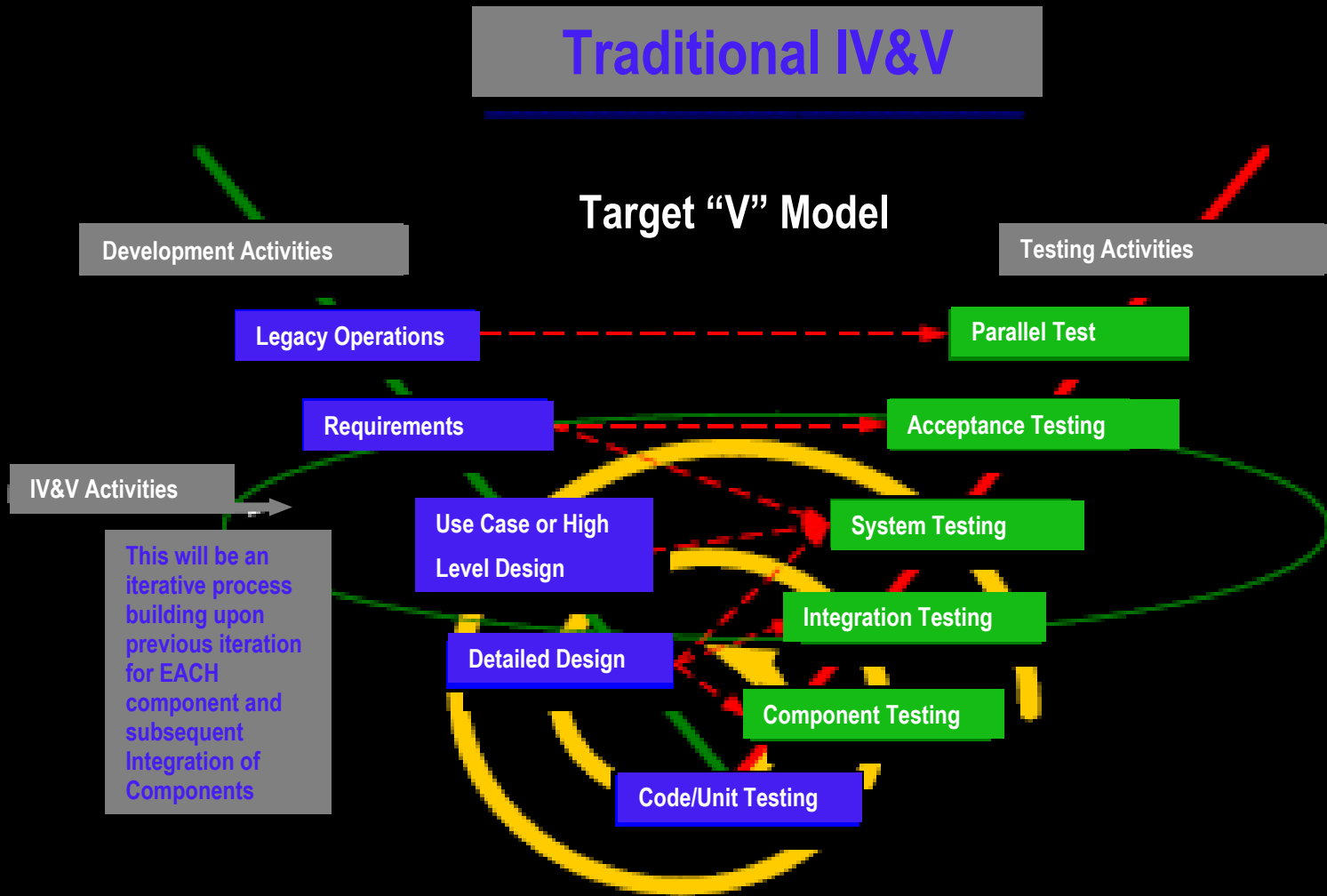
- ❖ **Learn design and dependencies of the parent systems**

- ❖ **Take time to understand applicable guidance**

System / Enclave / Enterprise



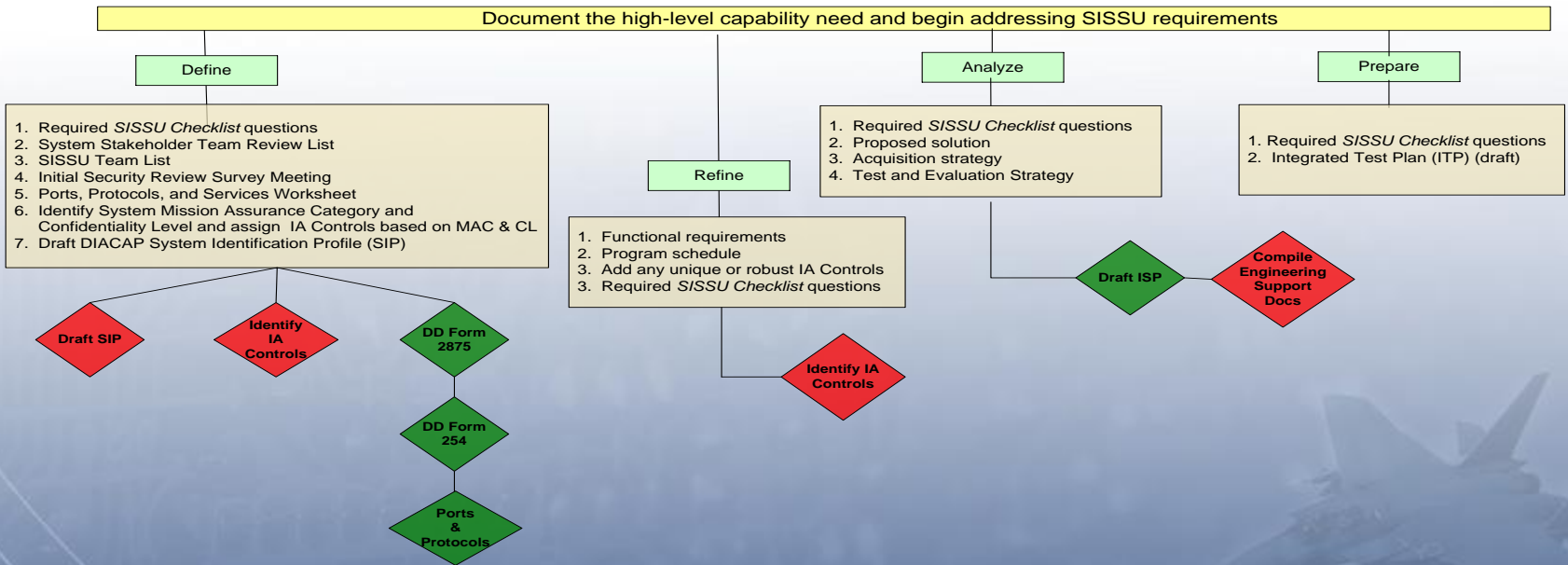
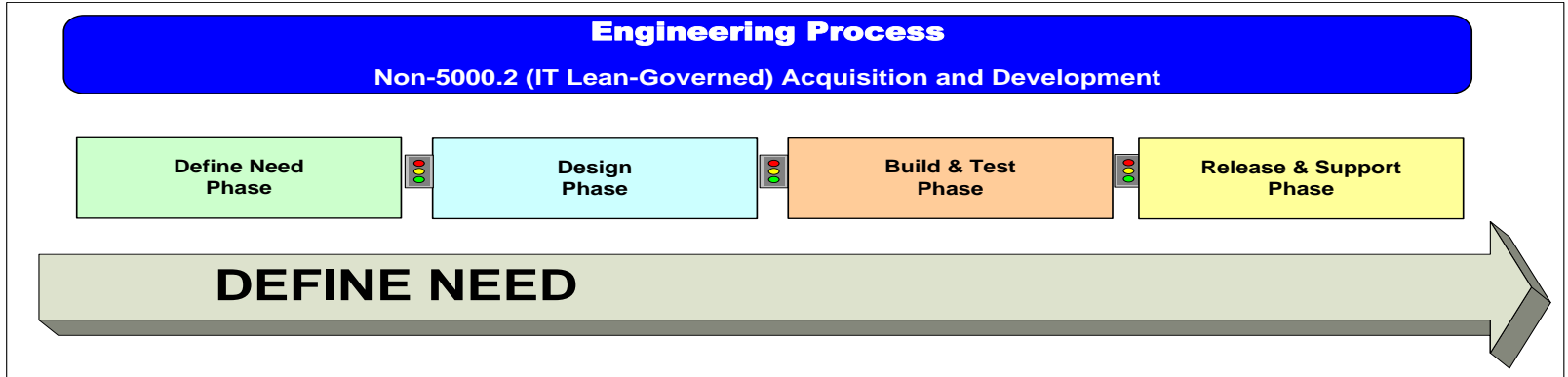
Traditional IV&V

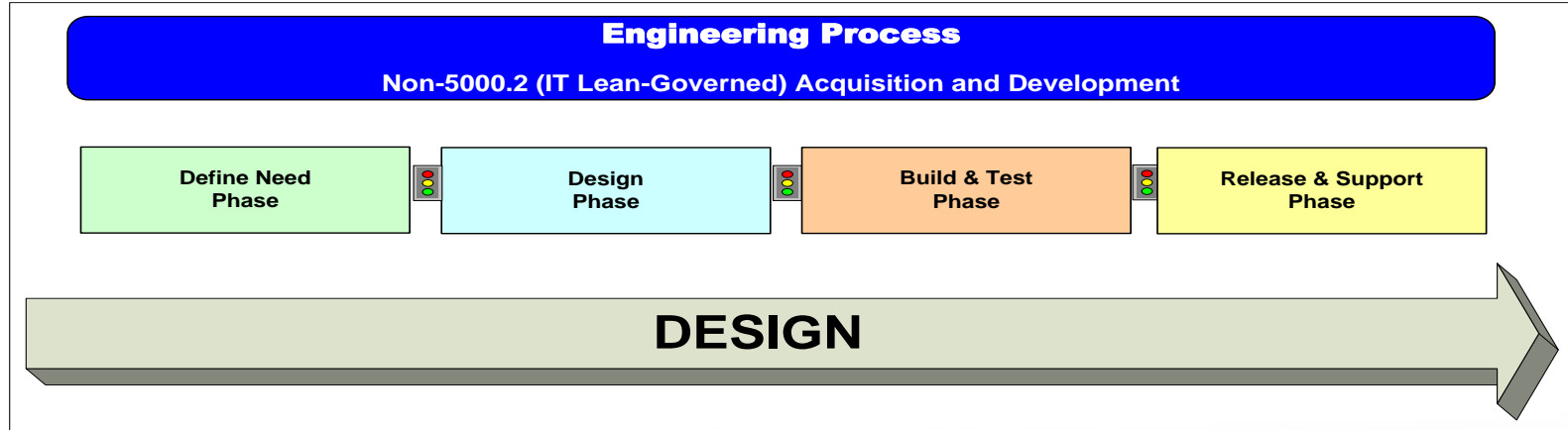


**How is this implemented in the
Department of Defense?**

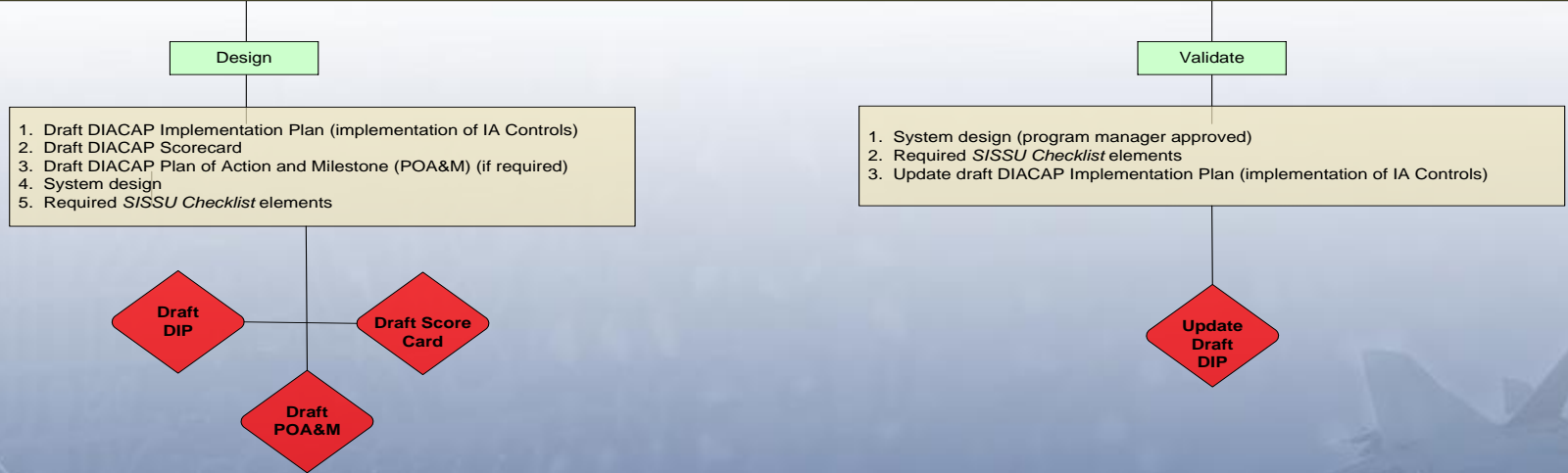


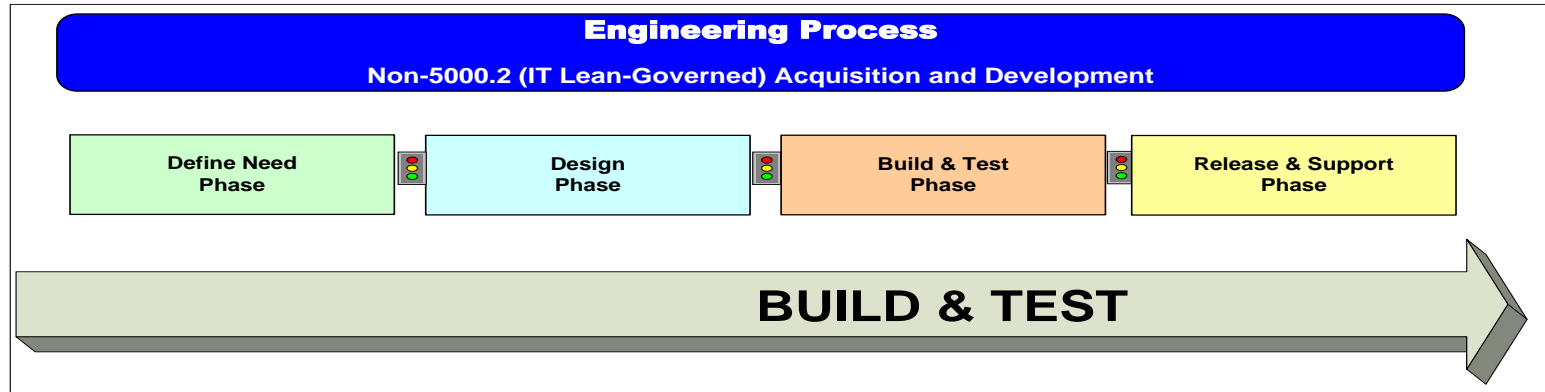
- ❖ **Currently 157 IA Controls – applicable based on system Mission Assurance Category (MAC) and Confidentiality Level (CL) (at the 1.1 level)**
 - Anywhere from 0 to 11 sub entries, depending on the control
 - Relative weighting of controls based on MAC
- ❖ **Almost all IA Controls require artifacts for supporting documentation**
- ❖ **Identification of appropriate IA controls automatic in EITDR**
- ❖ **Acceptability of risks and applied artifacts point of negotiation with DAA and AFCA**
- ❖ **SISSU Checklist identifies data to be captured**
- ❖ **Data entered to SISSU and EIDTR**
- ❖ **SIP, DIP, POA&M and ScoreCard generated by EITDR**



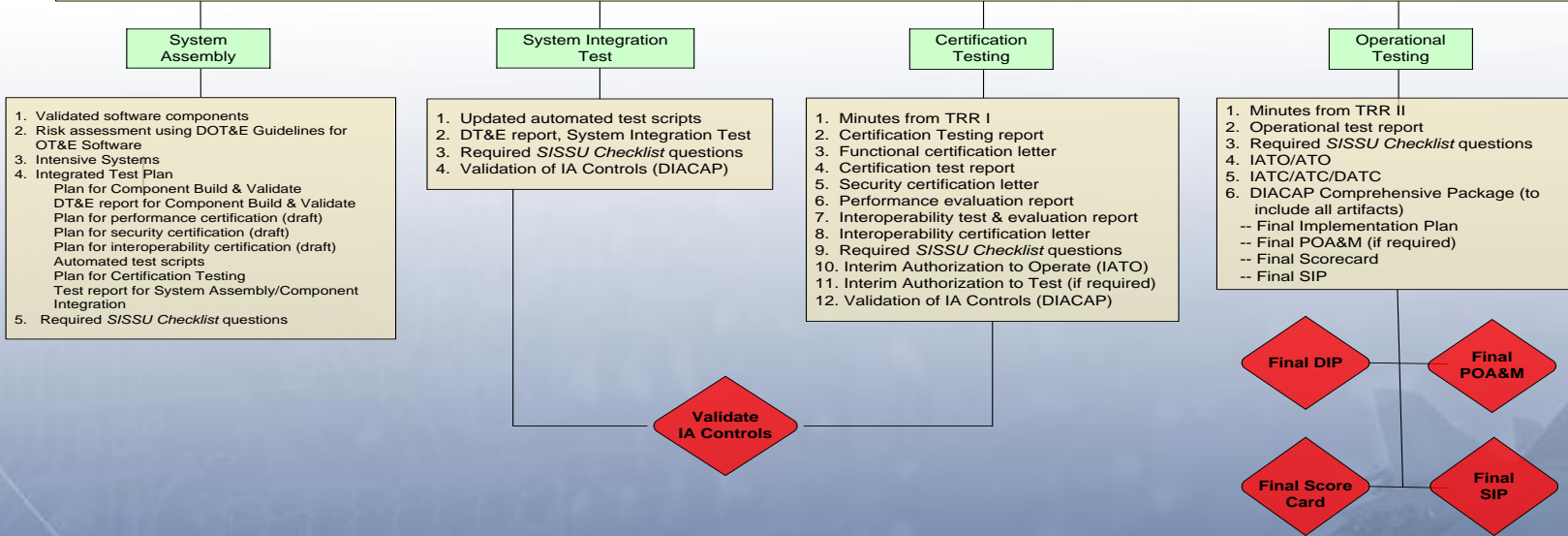


Design a solution consistent with the acquisition strategy

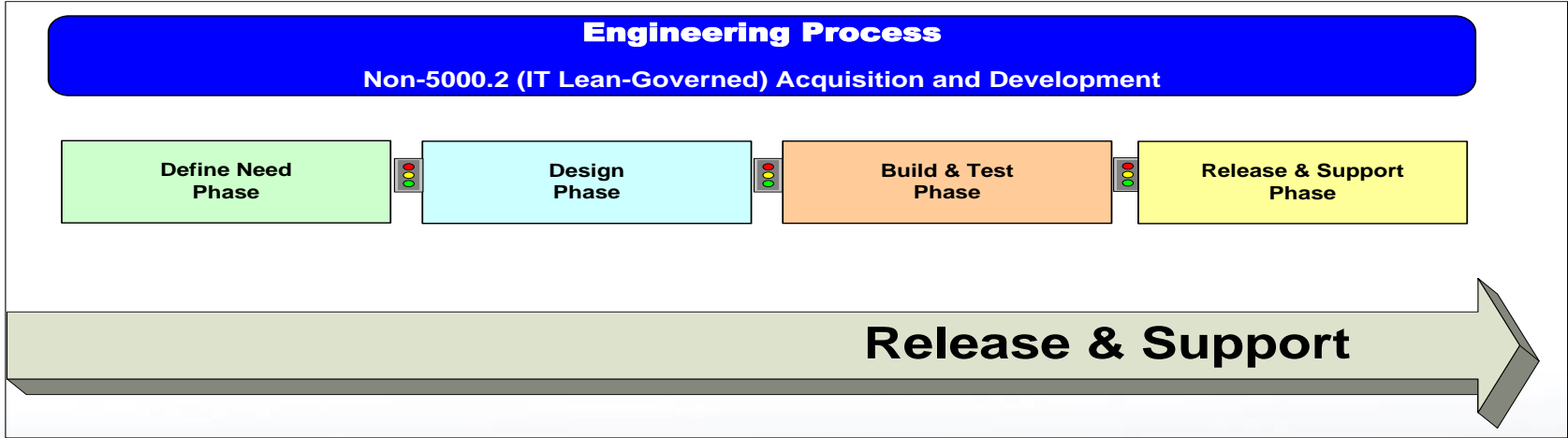




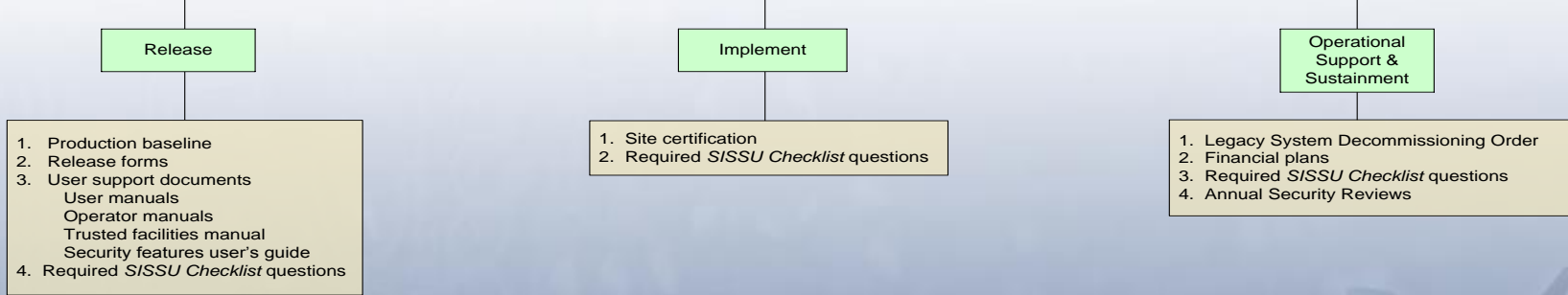
Represents the development, testing, and final review or approval activities of the system



IT Lean / SISSU Phase 4, Release & Support



This phase is triggered by the Field Readiness Review (FRR)



Questions.....?

Engility POCs for follow-up information:

Carmine F. Vilardi
Director, Mgm Operations
334-277-1972 ext 223
carmine.vilardi@engilitycorp.com

“Rick” Wilkison
Deputy Director, Mgm Operations
Chief IA COE
334-277-1972 ext 231
frederick.wilkison@engilitycorp.com

John Clements
Technical Director
334-277-1972 ext 240
john.clements@engilitycorp.com