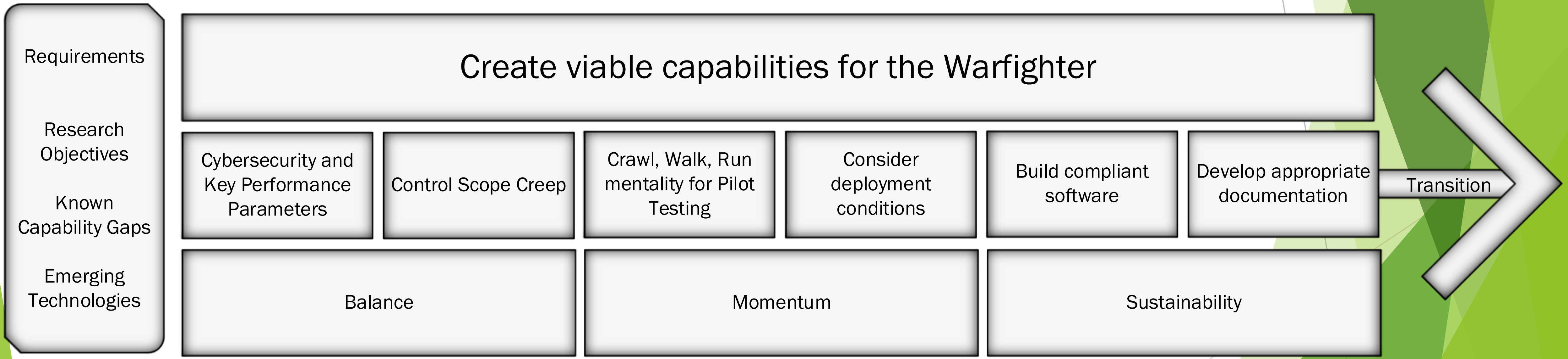
Cybersecurity and Research Projects

Mr. Mike Hernandez

Mr. Michael Neeley

BLUF

- BALANCE cybersecurity with research to conserve MOMENTUM moving through Technology Readiness Levels (TRL) and accreditation to ensure SUSTAINABILITY over a research program's lifecycle and potential transition



Requirements

Research Objectives

Known Capability Gaps

Emerging Technologies

Create viable capabilities for the Warfighter

Cybersecurity and Key Performance Parameters

Control Scope Creep

Crawl, Walk, Run mentality for Pilot Testing

Consider deployment conditions

Build compliant software

Develop appropriate documentation

Transition

Balance

Momentum

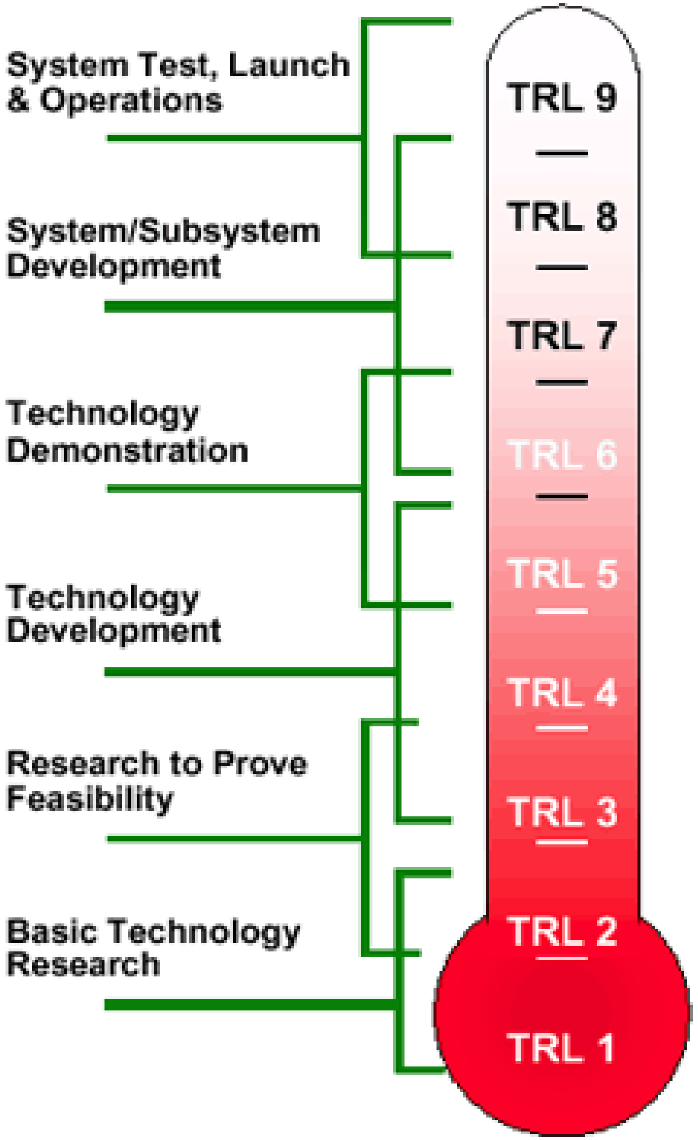
Sustainability

Topics

- Scope
- Research Project Management Primer
- Cybersecurity Primer
- Building for Transition
- The "Valley of Death"
- The "How" of Balancing Research and Cybersecurity
- Discussion
- References

Scope

- This presentation is focused on research programs related to the DoD
- Specifically, Advanced Technology Development(ATD)
  - (Budget Activity 3) RDT&E funding includes efforts that have moved into the development and integration of hardware/software for field experiments and tests (TRL 4,5,6)


System Test, Launch & Operations
System/Subsystem Development
Technology Demonstration
Technology Development
Research to Prove Feasibility
Basic Technology Research
TRL 9
TRL 8
TRL 7
TRL 6
TRL 5
TRL 4
TRL 3
TRL 2
TRL 1

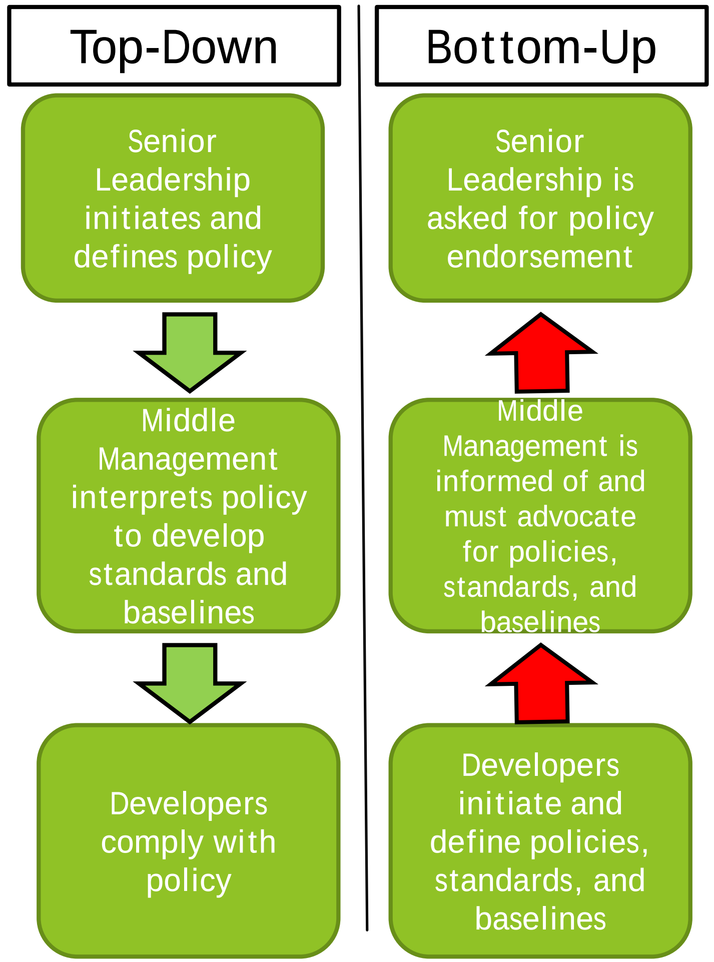
Research Project Management Primer

- Advanced Technology Development research is meant to demonstrate systems and sub-systems that have a direct relevance to identified military needs
- Investments at this level of research do not necessarily lead to subsequent development or procurement phases
- Programs should be event driven with schedules updated often to reflect actual progress
- For a transition to be successful, the software development associated with the capability must efficiently use its funding through its project lifecycle
  - Traceability is key from the research question to the delivered prototype.
  - Supports that a concept is **valid** and **valuable** to the DoD for transition into a Program of Record (PoR)

Cybersecurity Primer

- Cybersecurity up-front and early
  - Leadership setting goals and expectations lends credence to the endeavor
  - This concept spans all industries (MEDICAL, DOD, FINANCE…)
  - SD3+C (Secure by Design, Secure by Default, Secure in Deployment, Communications) -Microsoft
- Holistic view is required to gain true understanding of the system under test
  - Static and dynamic testing
  - Compliance monitoring and scanning
  - System and vulnerability scanning
  - Internal penetration testing

Top Down = Proactive
Bottom Up = Reactive



Top-Down

Senior Leadership initiates and defines policy

Middle Management interprets policy to develop standards and baselines

Developers comply with policy

Bottom-Up

Senior Leadership is asked for policy endorsement

Middle Management is informed of and must advocate for policies, standards, and baselines

Developers initiate and define policies, standards, and baselines

Build For Transition

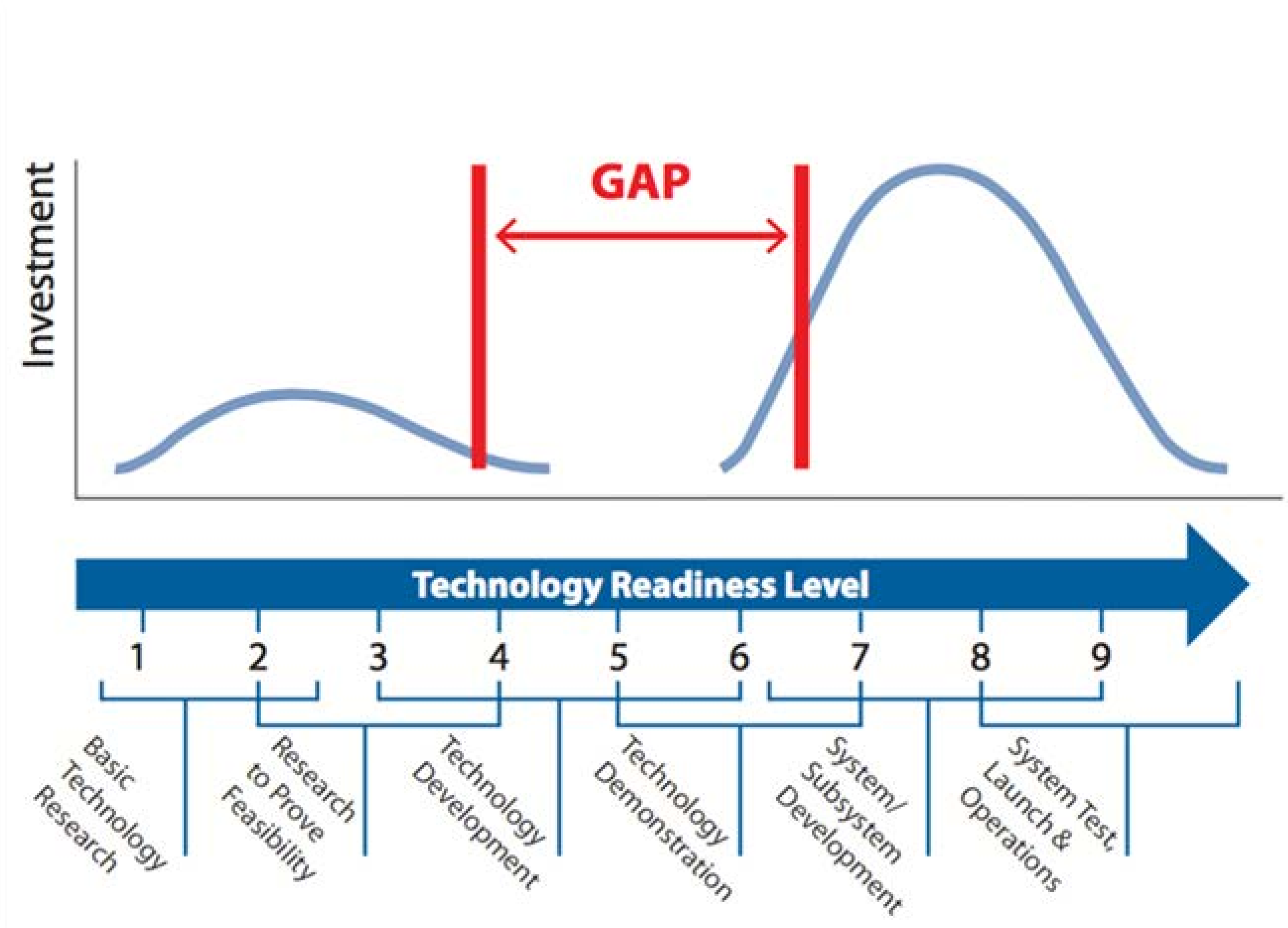
Avoid the Valley of Death

Preparing for Success as Early as Possible

- Think about READINESS
  - What will the research do for the Warfighter?
  - How is the demonstration during the research project proving it actually has value?
  - Can the things that get built actually be used by someone else?
- Think about your audience
  - Connect with the Warfighter by understanding their requirements, culture, and processes
- Pitfalls
  - Schedule overcoming potential
  - Are you prioritizing and planning to fix what you find?
  - Licensing
  - Unsupported open-source software
  - Data Rights

TRL Levels and the Valley of Death

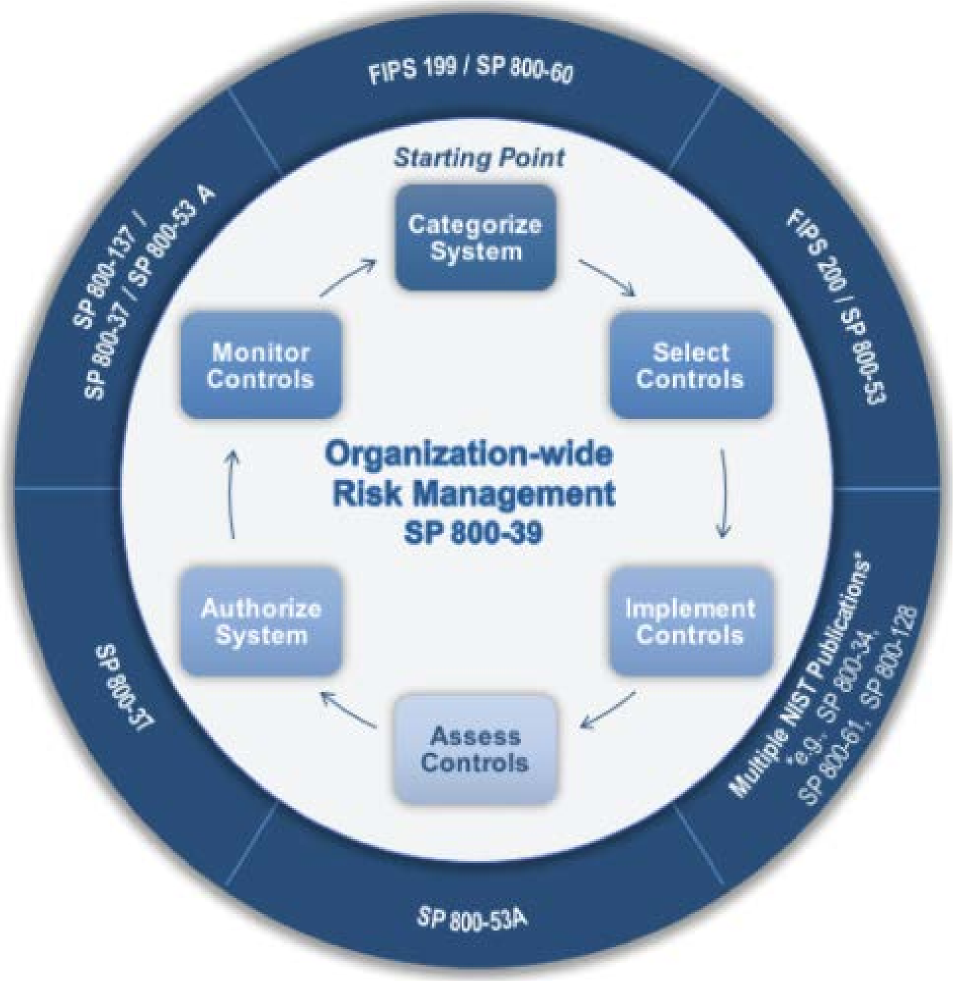
- Research projects have a known challenge moving beyond prototype to production
- Build a roadmap that increases quality and demonstrates capability at every step
- Sponsors have to see potential and build relationships with end-users
- Sponsors must think about funding, knowledge management, and transition from the start


Investment
GAP
Technology Readiness Level
1
2
3
4
5
6
7
8
9
Basic Technology Research
Research to Prove Feasibility
Technology Development
Technology Demonstration
System/ Subsystem Development
System Test, Launch & Operations

-"Universities are Wellsprings of Innovation, Drivers of Regional Economies"
Deborah Wince-Smith, Feb 2017

NIST and RMF

- National Institute of Standards and Technology (NIST) developed the Risk Management Framework (RMF)
  - A standard for securing information systems. Adopted as a standard by DoD
  - *DoDI 8510.01:* Risk Management Framework (RMF) for DoD Information Technology (IT) states that "All DoD IT that receive, process, store, display, or transmit DoD information will be managed through the RMF… "
  - DoD adoption of Risk Management Framework encourages research projects to tailor early and evaluate often



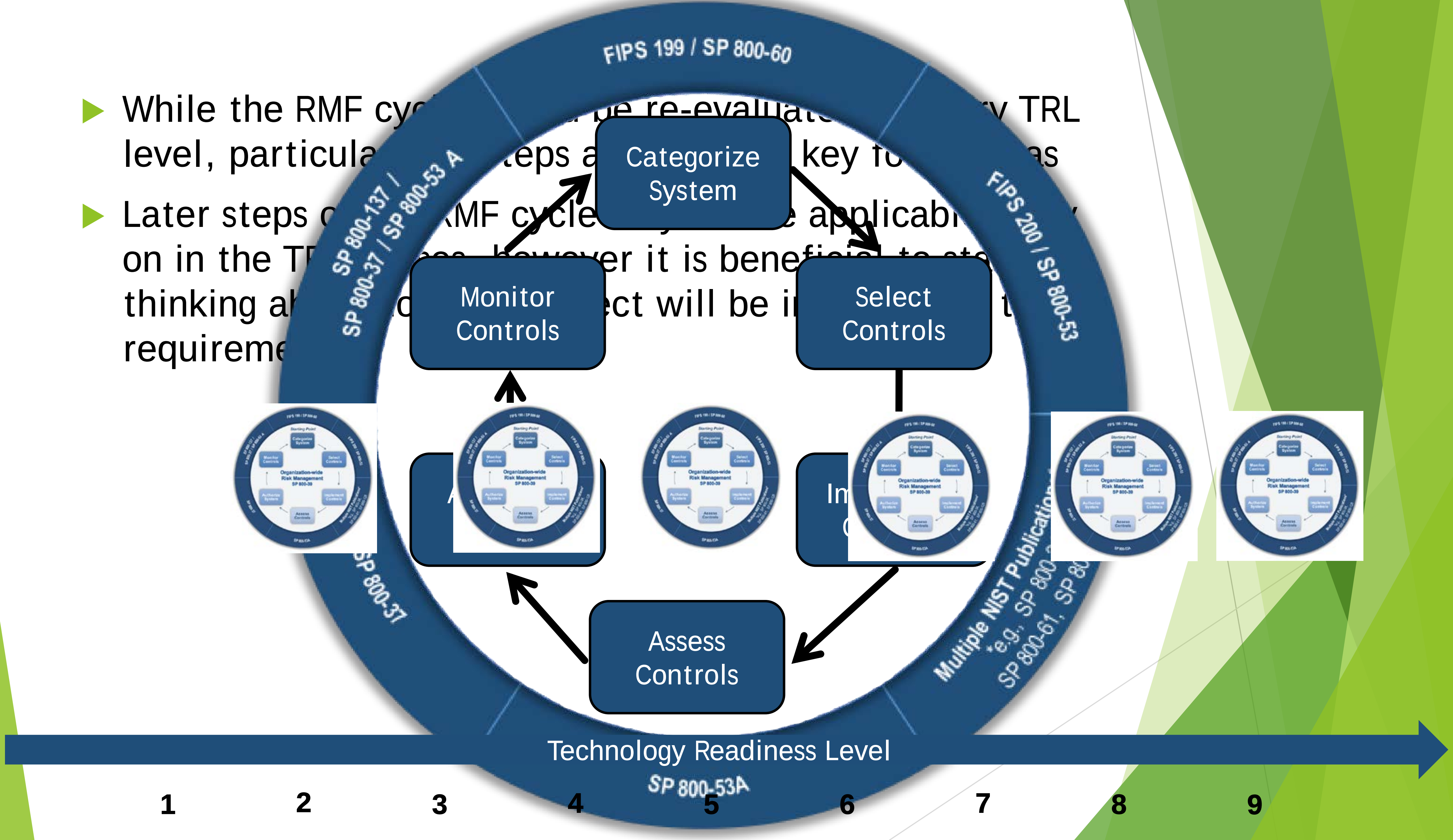
Risks and Impacts of Poor Cybersecurity Planning

- If you don't plan for RMF then transition will be harder, slower, and more expensive for DoD
- Code scanning and vulnerability assessment started later in the development process leads to a larger workload and more code refactoring
  - Fast paced projects initially use Feature Driven or Rapid Application Development methods, which prioritize functionality early
  - Without early planning for cybersecurity requirements, conflicts can arise with unsupported libraries / applications, controls, etc.
- Projects that transition may have funds for new function, but not yet for maintenance, leading to stale, non-compliant code while attempting to attain or maintain an Authority To Operate (ATO)

Tools for Implementing and Maintaining Cybersecurity Compliance

- Static Code Analysis Tools
  - Identify issues and vulnerabilities before they become a long term problem
- Compliance and Monitoring Tools
  - Security Content Automation Protocol (SCAP) Compliance Checker (SCC) analyzes and identifies DoD compliance shortfalls. This is useful for developing programs to test against a compliant environment for conflicts of software and system
- Vulnerability Scanning Tools
  - Identify required patches and vulnerabilities in your system
- Documentation
  - RMF documents are living documents and should grow with the project. Start early, update regularly
  - System Security Plan; Ports, Protocols and Services; Architecture Diagrams

- While the RMF cyc be re-evaluat y TRL level, particula teps a key fo as
- Later steps o RMF cycle e applicab y on in the TR es, however it is beneficial to sta thinking ab o ect will be in t requireme



Closing Statement

- From basic research to production, projects must benefit the Warfighter
- Spread the cost of cybersecurity across the software development lifecycle
- Cybersecurity investments have value beyond the software, they simplify adoption of good research into practice
- BALANCE cybersecurity with research to conserve MOMENTUM moving through TRL levels and accreditation to ensure SUSTAINABILITY over a research program’s lifecycle

Discussion

Resources

- RMF Guide
  - https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-Quick-Start-Guides
- Financial Guidance (US Navy)
  - http://www.acqnotes.com/Attachments/Financial%20Management%20Compendium%20June%202009.pdf
- DARPA Transition Guide
  - https://www.darpa.mil/attachments/DARPATransitionGuideFinal2-26-16.pdf
- A Manager's Guide to Technology Transition In an Evolutionary Acquisition Environment: *A Contact Sport*
  - https://www.acq.osd.mil/dpap/Docs/RandD%20Text.doc
- Valley of Death
  - https://blog.thegfcc.org/universities-are-wellsprings-of-innovation-drivers-of-regional-economies-8a3c097e6cc
- TRL Levels
  - http://acqnotes.com/acqnote/tasks/technology-readiness-level
- RMF
  - https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview
- SCA
  - https://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html