State of South Carolina

Professional Development Program (PDP)

Kevin Paul, Assistant Director, SC Division of State Human Resources

Alex White, Deputy Chief Privacy Officer, SC Enterprise Privacy Office

Tara Mahoutchian, Manager, Deloitte Consulting, LLP

November 2016

Contents

Background

The State of South Carolina (State) identified the need for a Professional Development Program (PDP) in order to help increase security posture enterprise-wide. This is especially important considering the State's federated model for InfoSec and Privacy.

Issues Driving the Need for a PDP

- Threats to InfoSec continue to grow in number and sophistication
- Increasing dependence on a knowledgeable InfoSec and Privacy workforce to combat potential risks and threats
- Increased need for non-InfoSec or Privacy staff at all levels to understand their role in protecting information assets
- Lack of human capital programs to support the InfoSec and Privacy workforce
- InfoSec and Privacy initiatives managed individually by State agencies, including governance

Implications of PDP

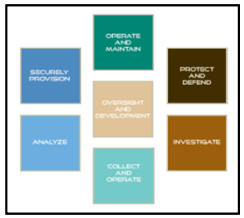
Strengthened security posture for the State by addressing the professional development of its InfoSec and Privacy personnel through:

- Defined roles and responsibilities;
- Role-based training (RBT) commensurate with the roles for individuals with significant security responsibilities (SSR), and
- Career growth options for InfoSec and Privacy professionals within the State.

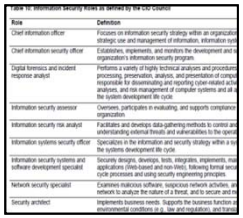
Considerations and Proposed Framework

We used a comprehensive approach to define InfoSec and Privacy critical roles and their associated responsibilities by referencing the National Initiative for Cybersecurity Education (NICE) framework, aligning with the State's data classification requirements and associated regulations, and other sources listed below.

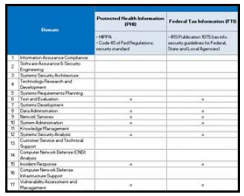
Authoritative Sources



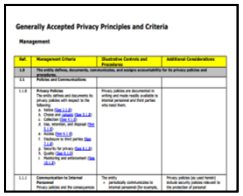
NICE Framework



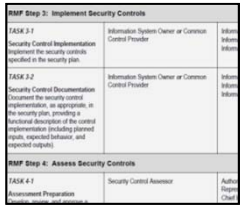
Federal Chief Information Officers (CIO) Council; Privacy Committee



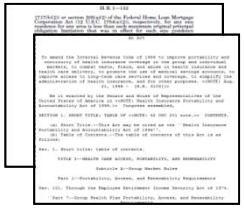
State Data Classifications Schema



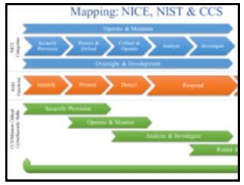
Generally Accepted Privacy Principles (GAPP)



NIST Special Publications (e.g., 800-53, 800-16, 800-37, 800-50)



HITECH, HIPAA



NIST Council on CyberSecurity (formally the National Board of Information Security Examiners)

Privacy Act of 1974

Proposed Framework

33 Skill Areas

11 InfoSec and Privacy roles

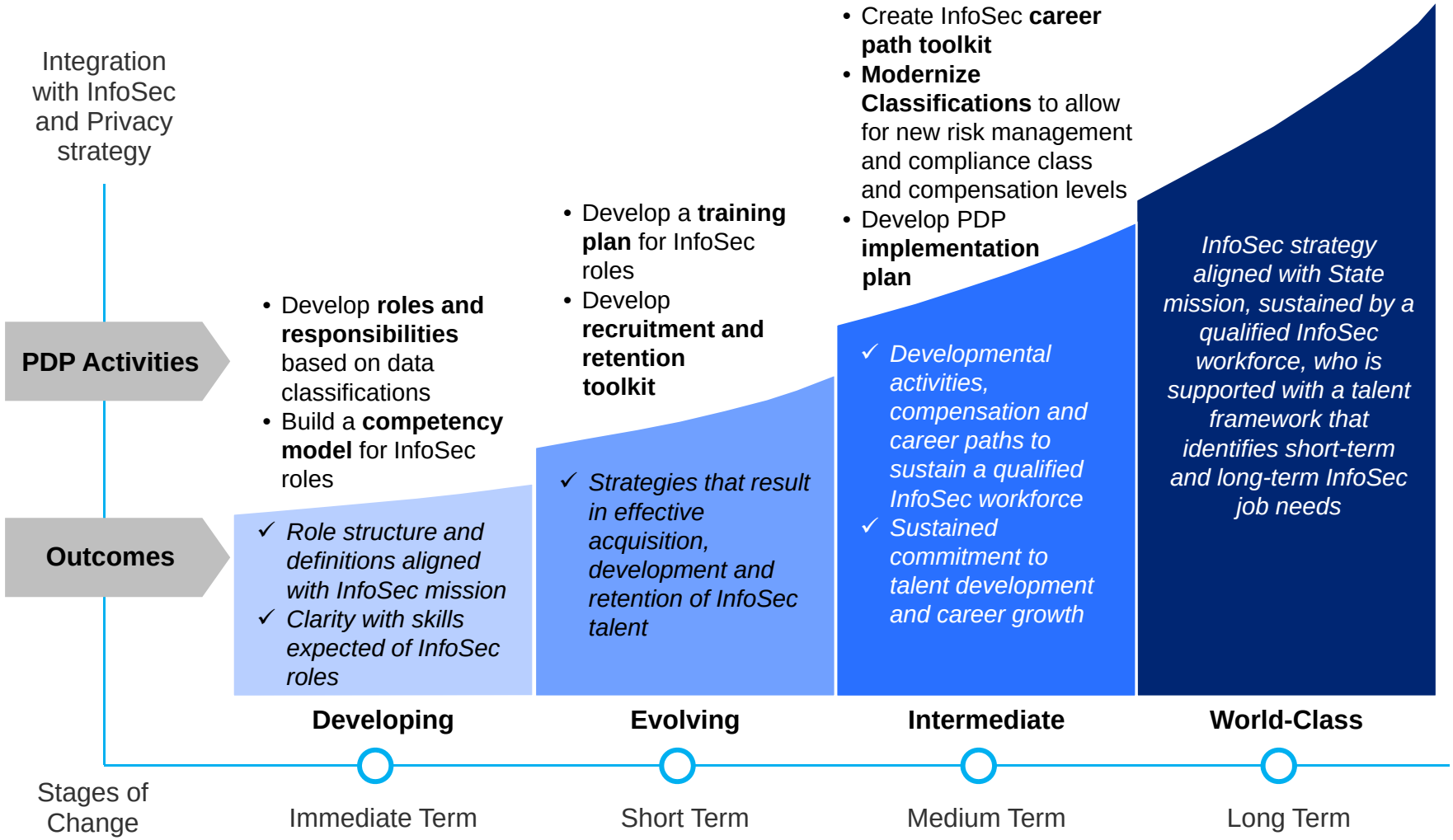
Role Definitions

Rationale for Framework

- Aligns with the National Institute for Standards in Technology's (NIST) NICE Framework
- Approaches InfoSec domains with a more holistic view beyond the data classifications and types associated with State and agencies
- Provides consistency with prior work completed with the State (e.g., skills assessment) and documentation already shared with agencies

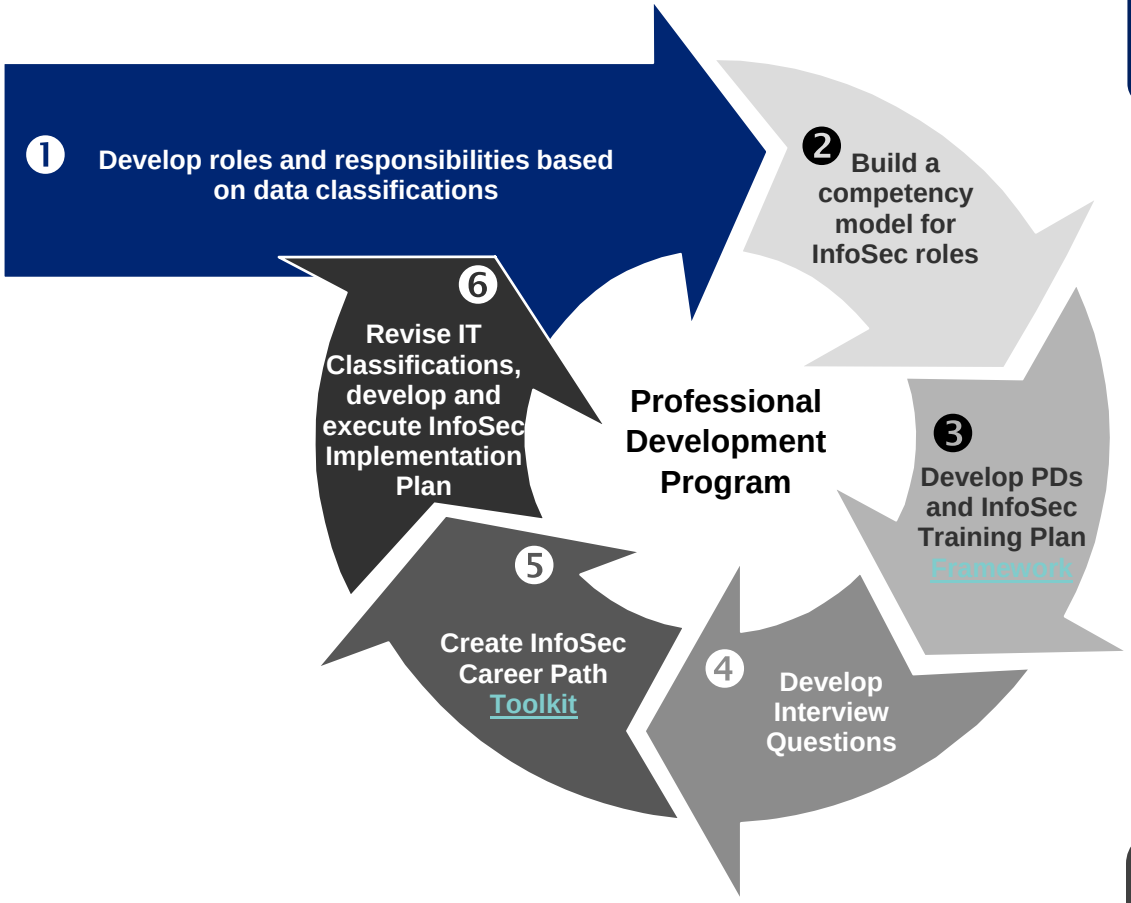
Expected Outcomes

Engaging in development of a PDP helps the State address InfoSec and Privacy workforce gaps and establishes the foundation needed to successfully execute and sustain the state's InfoSec and Privacy strategy.



Approach

The State took a holistic approach to InfoSec workforce planning and development by engaging in the below activities to develop workforce maturity;

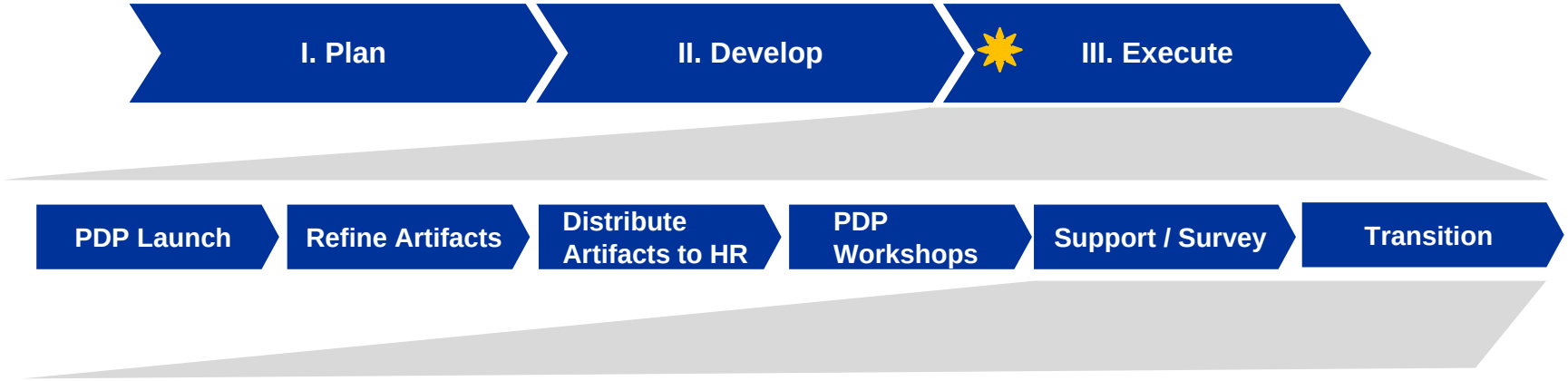


Activity outline:

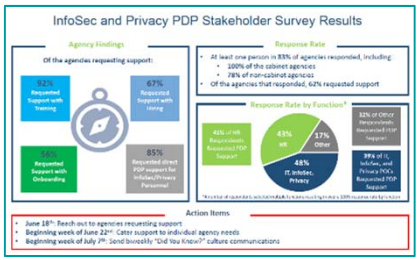
1. Defined **roles and responsibilities** aligned with the State's data classification requirements and associated regulations
2. Developed a **competency model based on NICE** that describes the skills, abilities and knowledge needed to fulfill identified InfoSec roles
3. Designed **position descriptions (PDs)** to set performance expectations and a **training plan** that aligns courses against PDs and the competency model for both core and non-core InfoSec and Privacy professionals
4. Developed **technical interview questions for PDs** to allow for more effective recruitment of new InfoSec and Privacy staff
5. Prepared a **career path toolkit** that outlines career options available to critical InfoSec roles
6. Revised IT Classifications and executed an **implementation plan** to engage InfoSec, Privacy, and HR to deploy the PDP Statewide, tailoring messages based on Agency needs

Implementation

A strategic, consistent, and pragmatic approach is pivotal to managing the success of PDP adoption. Our approach leverages existing infrastructures and processes with industry best practices for a successful adoption of the InfoSec and Privacy PDP.



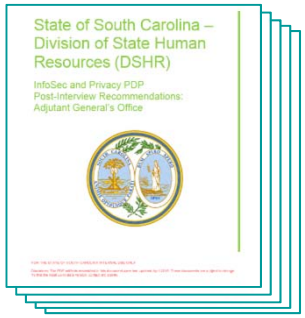
PDP Stakeholder Survey Results



InfoSec and Privacy Tips

PDP Adoption Tips

Follow-Up Recommendations



Survey Results and Outreach Status

Project Launch → Refine Artifacts → Distribute Artifacts to HR → PDP Workshops → Support / Survey → Transition

Agency Findings

Of the agencies requesting support:

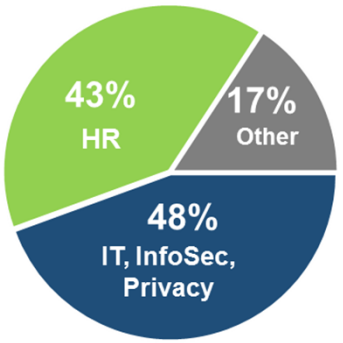
- **88%** Requested Support with Training
- **58%** Requested Support with Hiring
- **44%** Requested Support with Onboarding
- **78%** Requested direct PDP support for InfoSec/Privacy Personnel

Response Rate

- **127** total individual responses (**37%** response rate)
- At least one person in **83%** of agencies responded, including:
  - **100%** of the cabinet agencies
  - **78%** of non-cabinet agencies

Response Rate by Function

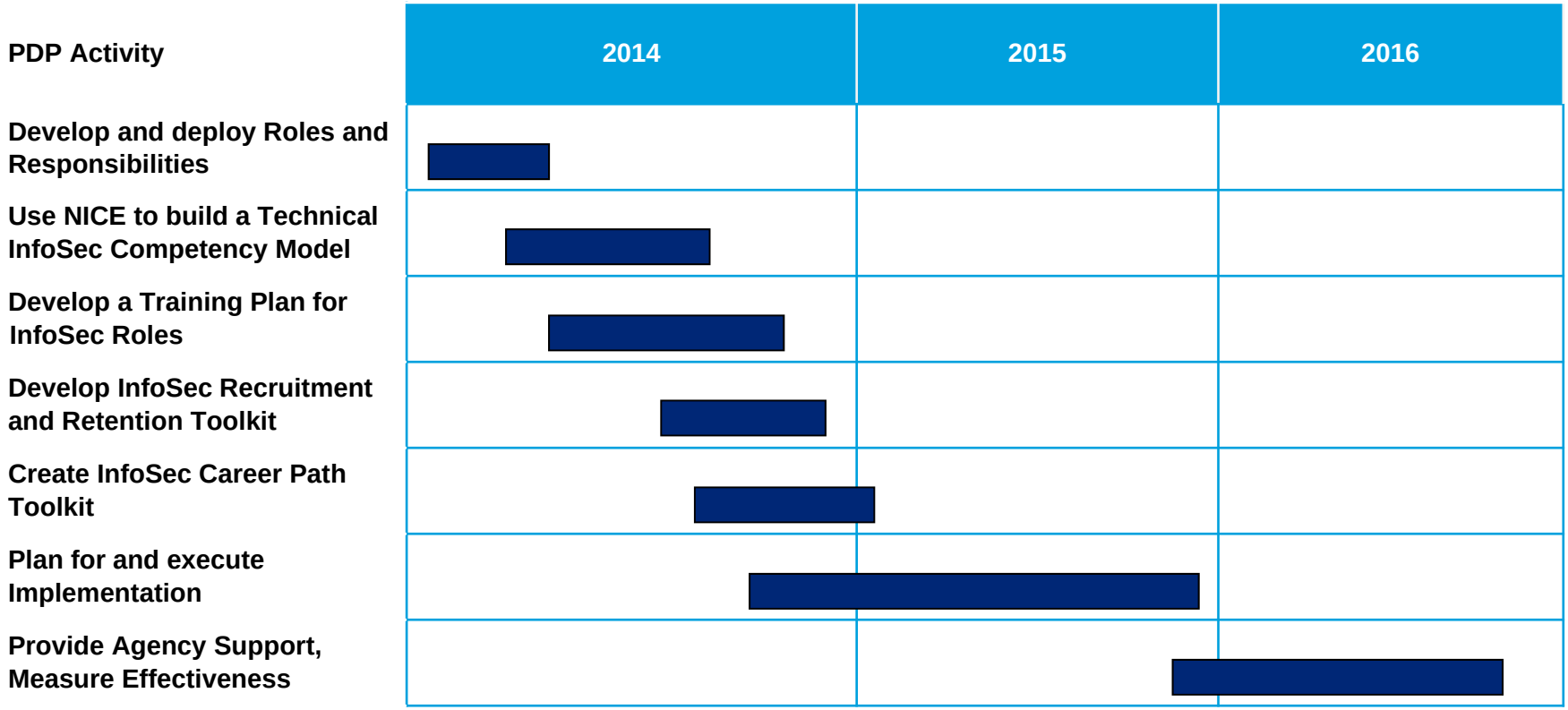
41% of HR Respondents Requested PDP Support



32% of Other Respondents Requested PDP Support

39% of IT, InfoSec, and Privacy POCs Requested PDP Support

Timeline



Measuring Effectiveness

The State of South Carolina's **Chief Information Security Officer Marcos Vieyra** stated that "the State of South Carolina's InfoSec and Privacy program consists of three pillars: people, process and technology. **The people component is by far the most important**; without people who can effectively perform InfoSec and Privacy duties, or who understand their role in the protection of State information assets, the program cannot be effective. **The PDP helps make sure that the right people with the right skills can implement the necessary processes and technology.** Through the deployment and continued maturation of the PDP, the State of South Carolina is at the forefront of developing a skilled InfoSec and Privacy workforce."

Points of Contact

For more information, please reach out to your panelists:

- Kevin Paul, Assistant Director, Division of State Human Resources: Kevin.Paul@admin.sc.gov
- Alex White, Deputy Chief Privacy Officer, Enterprise Privacy Office: Alex.White@admin.sc.gov
- Tara Mahoutchian, Lead. Cyber Risk People Solutions: tmahoutchian@deloitte.com

Q&A