

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

Considerations

Expected Outcomes

Approach

Timeline

Discussion





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

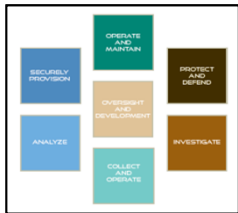
Implications of PDP

-  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

Role	Definition
Chief information officer	Focuses on information security strategy within an organization, change, use and management of information, information use.
Chief information security officer	Evaluates, implements, and monitors the development and management of information security program.
Digital forensics and incident response analyst	Performs a variety of digital forensic analysis and processes, including: investigation, analysis, identification of content, response, and management of computer systems and data, and the management of computer systems and data.
Information security assessor	Conducts, participates in evaluating, and supports compliance organization.
Information security risk analyst	Facilitates and develops data gathering methods to control and understanding information threat and vulnerabilities to the system, operations in the information and security strategy within a system, development the cycle.
Information systems security officer	Security design, design, build, integrate, implements and software development operations.
Network security specialist	Customize network software, response network activities, network to analyze the nature of a threat, and to secure and network.
Security architect	Implements information security, information and data.

Federal Chief Information Officers (CIO) Council; Privacy Committee

Domain	Personal Health Information (PHI)	Federal Tax Information (FTI)
1. Administrative and Operational		
2. Information Management		
3. Information Security		
4. Information Systems		
5. Information Technology		
6. Information Systems		
7. Information Systems		
8. Information Systems		
9. Information Systems		
10. Information Systems		
11. Information Systems		
12. Information Systems		
13. Information Systems		
14. Information Systems		
15. Information Systems		
16. Information Systems		
17. Information Systems		
18. Information Systems		
19. Information Systems		
20. Information Systems		

State Data Classifications Schema

Management	Information Security	Information Privacy
1.01	Information Security	Information Privacy
1.02	Information Security	Information Privacy
1.03	Information Security	Information Privacy
1.04	Information Security	Information Privacy
1.05	Information Security	Information Privacy
1.06	Information Security	Information Privacy
1.07	Information Security	Information Privacy
1.08	Information Security	Information Privacy
1.09	Information Security	Information Privacy
1.10	Information Security	Information Privacy

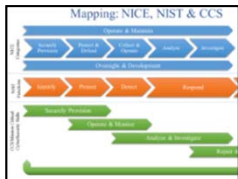
Generally Accepted Privacy Principles (GAPP)

Task	Information Systems Officer or Common Control Provider	InfoSec	Privacy
ISPK 2.1	Information Systems Officer or Common Control Provider	InfoSec	Privacy
ISPK 2.2	Information Systems Officer or Common Control Provider	InfoSec	Privacy
ISPK 4.1	Security Control Assessor	InfoSec	Privacy

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

Section	Section Title
1.01	Information Security
1.02	Information Security
1.03	Information Security
1.04	Information Security
1.05	Information Security
1.06	Information Security
1.07	Information Security
1.08	Information Security
1.09	Information Security
1.10	Information Security

HITECH, HIPAA

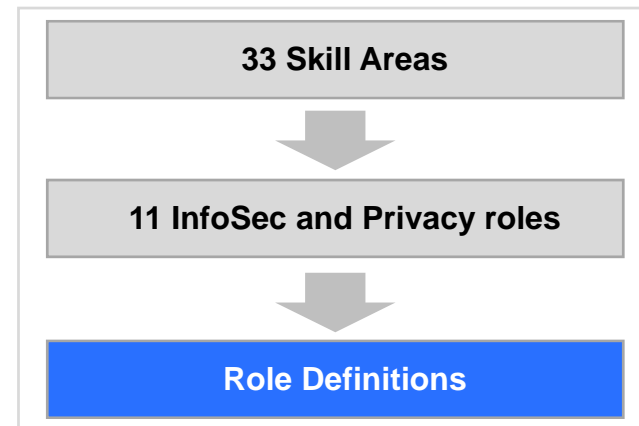


NIST Council on CyberSecurity (formerly the National Board of Information Security Examiners)

Section	Section Title
1.01	Information Security
1.02	Information Security
1.03	Information Security
1.04	Information Security
1.05	Information Security
1.06	Information Security
1.07	Information Security
1.08	Information Security
1.09	Information Security
1.10	Information Security

Privacy Act of 1974

Proposed Framework

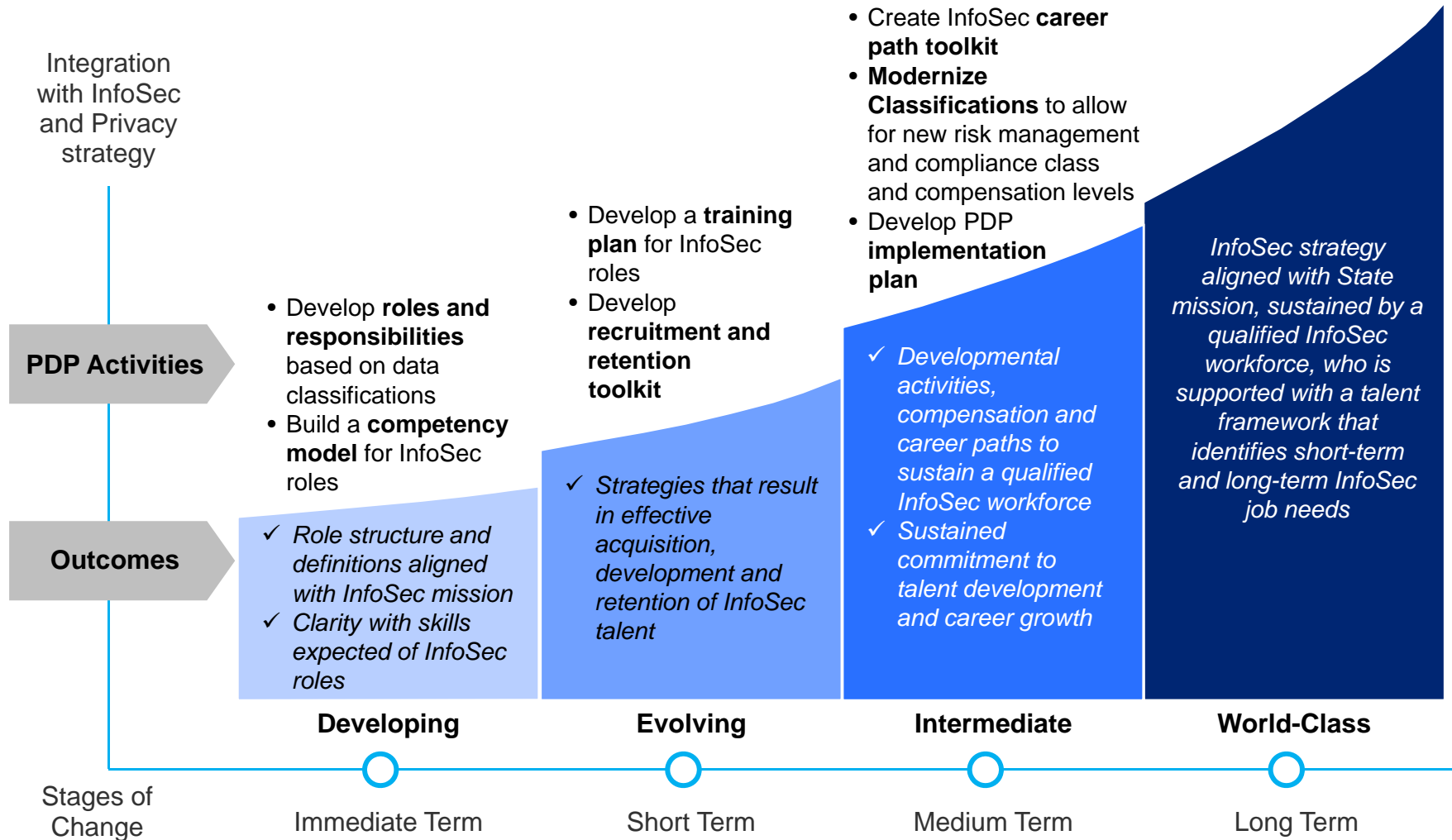


Rationale for Framework

- 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

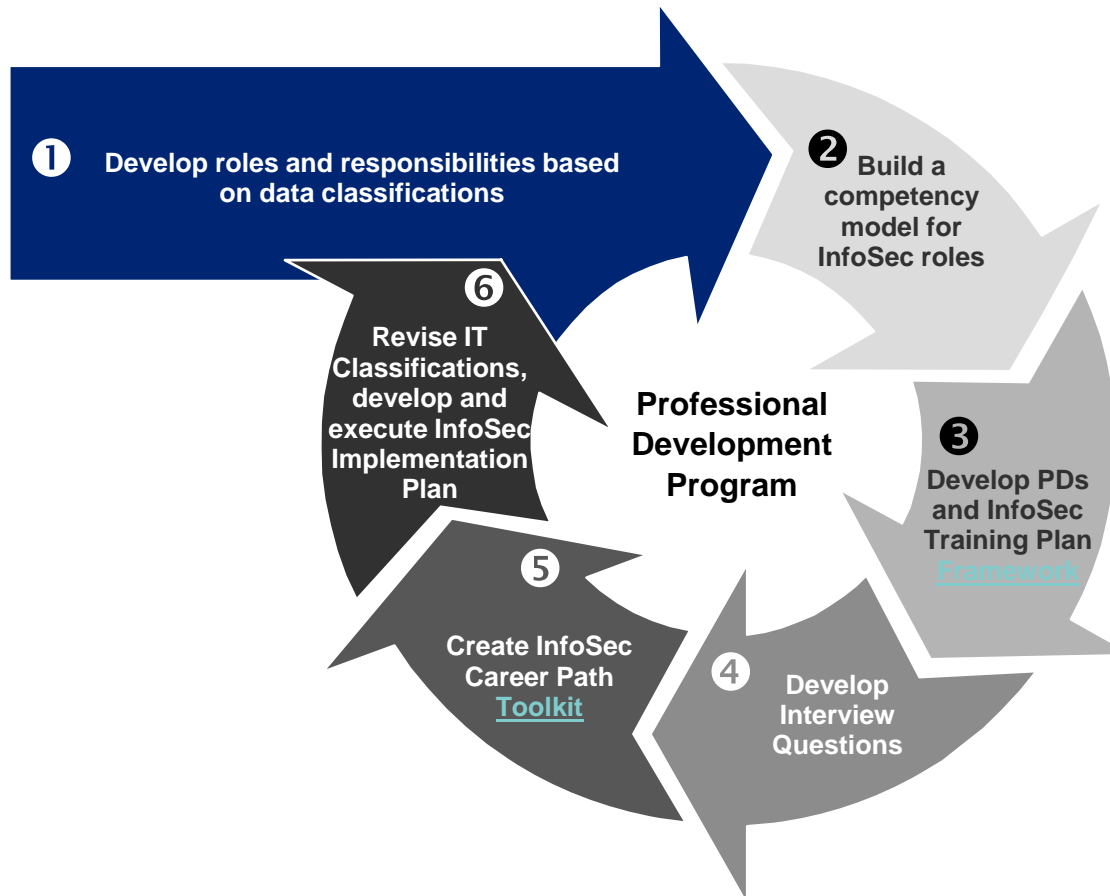
Expected Outcomes

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:

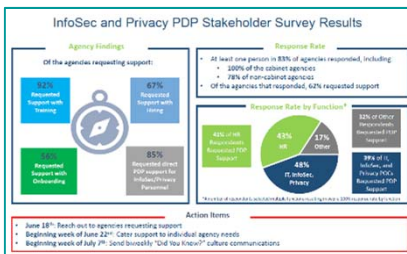
- 1** Defined **roles and responsibilities** aligned with the State's data classification requirements and associated regulations
- 2** Developed a **competency model based on NICE** that describes the skills, abilities and knowledge needed to fulfill identified InfoSec roles
- 3** Designed **position 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

Did you know?

In 2014 alone, 47 percent of American adults had their personal information exposed by hackers.

Good news! You can easily prevent this threat – every time you enter personal information in a web browser, make sure the URL begins with <https://> not <http://>. The **s** means the page is secure and the data you enter will be **encrypted**.

You can learn more about protecting your information at dis.sc.gov

InfoSec and Privacy PDP

PDP Adoption Tips

Looking to develop your InfoSec and Privacy personnel?

Use the resources attached to do the following:

1. Review the InfoSec and Privacy Training Requirements to identify training opportunities by competency, certification, and/or position description
2. Use the Career Path Guide to inform training decisions and conduct career progression discussions
3. Check the DIS website at dis.sc.gov periodically for DIS or EPO-provided training opportunities

Contact: jlambury@deloitte.com

Follow-Up Recommendations

State of South Carolina – Division of State Human Resources (DSHR)

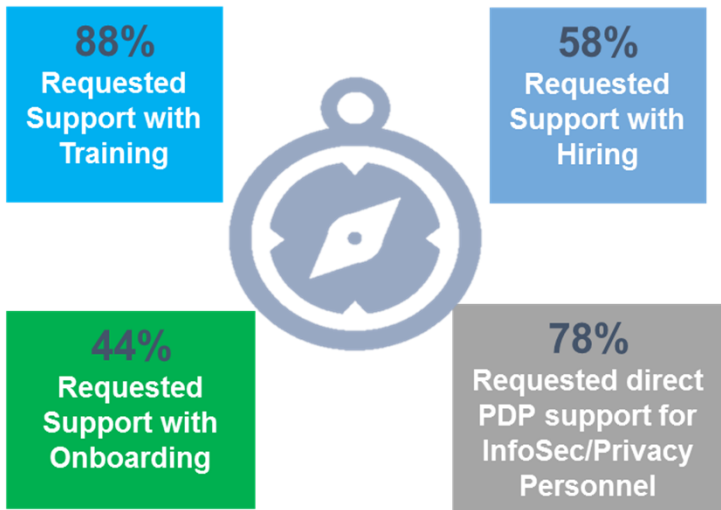
InfoSec and Privacy PDP Post-Interview Recommendations: Adjutant General's Office

Survey Results and Outreach Status



Agency Findings

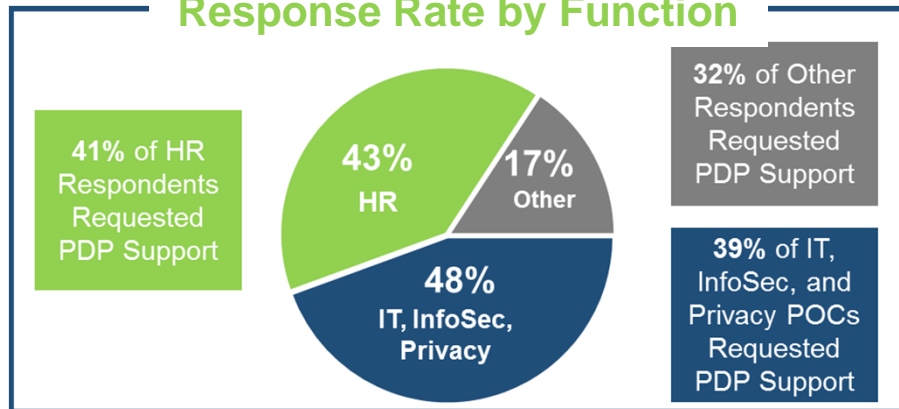
Of the agencies requesting support:










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



Timeline

PDP Activity	2014	2015	2016
Develop and deploy Roles and Responsibilities			
Use NICE to build a Technical InfoSec Competency Model			
Develop a Training Plan for InfoSec Roles			
Develop InfoSec Recruitment and Retention Toolkit			
Create InfoSec Career Path Toolkit			
Plan for and execute Implementation			
Provide Agency Support, Measure Effectiveness			

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
