

State of South Carolina – Human Resources Division

InfoSec / Privacy Workforce

Frequently Asked Questions (FAQs)



ABOUT THIS DOCUMENT

This document captures Frequently Asked Questions (FAQs) about the Information Security (InfoSec) and Privacy Professional Development Program (PDP) artifacts and deployment. This document follows a similar layout to the PDP handbook, allowing for ease of use and understanding. The FAQs address hiring, onboarding, continual learning and performance evaluation questions as they pertain to the InfoSec and Privacy workforce.

Employee FAQs

GENERAL

Q: When will I receive the artifacts for the PDP presented in the HR Workshops?

A: The PDP artifacts and reference materials were provided in initial communications. Some of the more relevant materials are posted to the Human Resources InfoSec & Privacy PDP web site and are available through the InfoSec & Privacy PDP Manager or your HR Consultant.

Q: When can I incorporate the artifacts for InfoSec and Privacy PDP?

A: You should incorporate the PDP artifacts immediately into existing InfoSec and Privacy talent practices (e.g., posting a new job requisition, training existing staff). It is expected that agencies will implement these artifacts, as needed, by July 2015.

Q: How often will the PDP artifacts be updated?

A: These artifacts will be periodically updated on a case-by-case basis, depending on relevant internal and external changes within InfoSec and privacy.

Q: How is adoption of the InfoSec and Privacy PDP tracked?

A: There is no State mandate to incorporate the tools provided within the PDP, and there is currently no plan to track its adoption, as levels of adoption will vary by agency. The PDP artifacts are meant to support your agency in development of your InfoSec and Privacy workforce.

Q: Are there plans to audit agencies in the adoption of the InfoSec and Privacy PDP?

A: The Division of Information Security (DIS), Enterprise Privacy Office (EPO), and Division of State Human Resources (DSHR) may conduct assisted walk-throughs to support agency adoption. The InfoSec & Privacy PDP Manager and HR Consultants are available to help with any questions.

Q: Is my Agency Director aware of the InfoSec and Privacy PDP?

A: Yes, details about the InfoSec and Privacy PDP were communicated to all Agency Directors through email notifications and memorandum. Additionally, HR Directors, IT Directors, Training Coordinators, InfoSec Liaisons, and Privacy Liaisons from all agencies were invited to attend PDP workshops to review key artifacts and tools available to support their agencies.

Q: Has the State procured any training courses for the InfoSec and Privacy workforce?

A: Yes, DIS and EPO procure training on an annual basis, budget allowing. You can find a list of trainings offered by DIS and EPO at <http://dis.sc.gov>. The courses are listed under Upcoming Events.

Q: Does the State have existing partnerships with training vendors?

A: Yes, DIS has partnered with the SANS Institute for the InfoSec workforce. The SANS Institute is a cooperative research and education organization and the largest

source for InfoSec training and security certification in the world. For more information on the SANS Institute, please visit: <https://www.sans.org/>.

EPO has partnered with the International Association of Privacy Professionals (IAPP) for the Privacy workforce. The IAPP is the world's largest global information privacy community and has resources available to professionals who want to develop and advance their careers managing Privacy risks and data protection. For more information on the IAPP, please visit: <https://privacyassociation.org>.

The InfoSec and Privacy Training Framework illustrates both SANS and IAPP trainings that may be applicable to InfoSec and Privacy personnel.

Q: What is the difference between InfoSec and privacy?

A: Whereas InfoSec is a mechanism to implement protections; privacy determines what information needs to be protected, to what extent it needs to be protected and from whom it needs to be protected.

InfoSec refers to the processes and methodologies, which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Privacy encompasses the analysis of policy and business processes to ensure the legal and ethical obligations of an organization are upheld when it collects, stores, uses and discloses sensitive information. This includes informing the public of information practices and providing opportunities to choose whether personal information will be shared, restricting access to information, and assessing risks associated with the unauthorized access to or loss of sensitive information.

Q: Are there any efforts to share InfoSec and Privacy resources for smaller agencies?

A: DIS is in the process of developing a Virtual Chief Information Security Officer (VCISO) model (pending legislative approval), where multiple agencies could share the resource based on agency needs. Additionally, agencies with current needs may be able to share resources independently via service level agreements.

EPO is available to discuss shared resources for Privacy personnel.

Q: What is a virtual CISO model?

A: A virtual CISO model allows a number of agencies to share a CISO, or equivalent resource. This resource would report to DIS, with oversight and governance authority of InfoSec for the participating agencies. This proposed shared services model is intended to limit agency hiring costs while simultaneously elevating the InfoSec and Privacy programs of each participating agency. The virtual CISO model is currently in development.

HIRING

Q: Are new classifications linked only to Information Technology (IT)?

A: The current IT classifications have been modernized to reflect additional roles that are not specifically IT aligned, including new areas such as Governance, Risk & Compliance (GRC).

A crosswalk will be provided to help guide you through the new classifications and how they align with existing classifications and new Position Descriptions (PDs). The new classifications should be updated at your agency by July 2nd, 2015.

Q: How do I apply the updated IT classifications to InfoSec or Privacy personnel?

A: Depending on their role, InfoSec personnel should be reclassified under the Security or Risk Management and Compliance IT domains. Privacy personnel should be classified under Risk Management and Compliance.

Q: How can I adopt the new classifications without any additional budget?

A: The introduction of new classifications was created in alignment with the current classification levels. Most IT professionals already fall within the established pay bands, thus allowing for budget-neutral changes when transitioning your agency to the new classifications.

Q: How do I know if I should hire an InfoSec or Privacy position in order to fulfill the InfoSec and Privacy roles and responsibilities?

A: The Roles and Responsibilities Toolkit can help agencies define its InfoSec and/or Privacy needs. The toolkit includes a tier categorization to help determine the recommended number of Full Time Equivalents (FTEs) to fill InfoSec and Privacy roles. It also includes a role-to-position map to illustrate how various positions may align to InfoSec and Privacy roles.

In many cases, there may not be a need to hire new personnel as existing agency staff may be able to adequately fill all InfoSec and Privacy roles. If an agency does identify a hiring need, the agency can leverage InfoSec and Privacy PDs to create a job posting and begin the hiring process. Each situation is determined by agency needs and requirements on a case-by-case basis.

Q: Are there certain criteria where Privacy employees would not report to the IT Director?

A: Determination of an employee's roles and responsibilities vary based on agency needs and requirements. Agencies should strive to maintain the segregation of duties outlined in the Roles and Responsibilities Toolkit. It is preferred, but not required, to have the roles be mutually exclusive.

Q: What is the difference between Core and Hybrid positions?

A: DIS, EPO, and DSHR have identified 12 unique positions that can perform the roles and responsibilities necessary to support InfoSec and privacy for the State. These include Core and Hybrid positions:

- Core positions are newly created positions, dedicated full-time to InfoSec and/or Privacy roles and responsibilities

- Hybrid positions are existing positions that have both InfoSec or Privacy and non-InfoSec or Privacy roles and responsibilities

Q: Am I limited to the Technical Interview Questions when interviewing job candidates?

A: The Technical Interview Questions are suggestions for topics that could be discussed during the interview process and are not a replacement for existing interview questions or processes.

It is recommended that the Technical Interview Questions be used as a supplement to screen candidates for the expertise and skills that are required for InfoSec and Privacy positions.

Q: Is there an answer key for the Technical Interview Questions?

A: Considering the sensitive nature of InfoSec and Privacy positions, it is in the best interest of agencies to not have an answer key for the Technical Interview Questions. Individuals conducting these interviews should have sufficient subject matter expertise for the position they are interviewing. If the interviewer reviews the Technical Interview Questions and determines that they do not have the requisite knowledge, they may reach out to DIS and EPO for direct support in the interview process.

Please reach out to DIS and EPO for further guidance.

Q: Should job candidates obtain all training certifications and coursework laid out in the Training Framework?

A: No, the Training Framework serves as a resource for continual development and performance evaluation. When evaluating a candidate for an open requisition, it is recommended that candidates demonstrate the knowledge, skills and abilities (KSAs) to successfully perform job duties as outlined in the PD. Preferred (but usually not required) certifications are also listed within each PD.

Q: How will the PDP Deployment impact recruiting efforts?

A: The State believes that deployment and adoption of the PDP should positively impact recruiting efforts. PDs will help attract more qualified candidates to the State for both external and internal hires. The training courses offered provide additional non-monetary incentives for prospective candidates to join the State. Further, increased training helps create a more knowledgeable and prepared workforce, thereby increasing the amount of internal candidates eligible for open positions within the State.

Q: Can employees completing the InfoSec and Privacy roles and responsibilities be in the same organization?

A: Yes, as long as the recommended separation of duties exists between individuals handling InfoSec and Privacy roles and responsibilities. It is important to maintain a clear separation of duties, instill checks and balances where possible, and eliminate potential conflicts of interest.

Q: My department currently only has one InfoSec/Privacy resource, how can I fulfill the new requirements without adding new staff?

A: Agencies can share support with other agencies and DIS/EPO where appropriate, depending on shared systems, agency locations, data sensitivity, and other factors. While roles can be shared across agencies, it is critical to ensure the minimum number of FTEs are filled based on each agency's tier.

DIS is proposing a virtual CISO model, which would allow various State agencies to share resources needed to fulfill the required InfoSec and Privacy roles and responsibilities without hiring new employees. The virtual CISO's time and resources will be allocated based on agency needs as determined by DIS.

ONBOARDING

Q: How can I effectively leverage InfoSec and Privacy PDP artifacts in the onboarding process?

A: Onboarding of newly hired employees, including setting performance expectations, is each hiring agency's responsibility. This includes defining annual performance goals, establishing mutual understanding of a clear career path, highlighting training opportunities, and identifying competencies essential to career progression. The Career Path Model and Competency Model help agencies onboard newly hired or transferred employees.

The Career Path Model is designed to help define various career options available to the State's InfoSec and Privacy workforce. It provides an overview of the InfoSec and Privacy career path, including opportunities for Technical and Management career progression.

The Competency Model outlines respective KSAs needed to fulfill the State's InfoSec and Privacy roles. It helps InfoSec and Privacy employees manage their own careers by providing them with a clear understanding of expected competencies for each InfoSec and Privacy domain.

Q: Will all InfoSec and Privacy personnel follow the same Career Path Model?

A: No, each career path is reviewed on a case-by-case basis with consideration to experience, training, competency-level, and current agency needs. Some agencies may not have a need for InfoSec or Privacy roles beyond existing positions. Transfers to different agencies may be necessary for InfoSec and Privacy career progression.

This Career Path Model can help provide new hires with insight into a long-term career path upon joining the State, serving as reference for potential vertical and lateral career moves.

Q: Where can I find the Privacy Technical Expert career path?

A: As privacy continues to advance in maturity and opportunities become available, a Privacy Technical Expert career path could be created for Privacy personnel.

Q: Is the Competency Model inclusive of all mandatory requirements?

A: The Competency Model outlines respective KSAs needed to fulfill the State's InfoSec and Privacy roles. The Competency Model enhances State HR or talent practices, including training curriculum development and professional development planning.

While the Competency Model strives to include all requirements today, it may need to be modified as InfoSec and Privacy requirements change over time.

CONTINUOUS LEARNING AND PERFORMANCE EVALUATION

Q: What is the end goal of the training provided by the State?

A: The State is providing extensive training to employees in order to attract and retain top talent. Having an educated and trained workforce will help the State elevate its InfoSec and privacy posture and to more effectively protect State and citizen information assets.

The Training Framework helps inform agencies about the relevancy of courses requested by employees (or their supervisors) in order to increase their proficiency and help protect the State's information assets.

Q: Is there a list of all the training courses procured?

A: Yes, a list of all training courses can be found on <http://dis.sc.gov>. The site is continually updated to reflect InfoSec and Privacy courses offered by the State.

Q: Are the training courses presented in the Training Framework internally provided by the State?

A: Most of the courses provided are external, available for purchase through various training providers. Most of the trainings are offered by top organizations such as SANS, IAPP, and ISACA, among others, who excel in InfoSec and Privacy training.

Q: Can the InfoSec and Privacy PDP artifacts be leveraged for a skills assessment?

A: Yes, the InfoSec and Privacy Competency Model was specifically designed for inputs into several talent management practices, including technical skills assessments.

Q: Will there be any changes to Performance Evaluations based on the adoption of the new InfoSec and Privacy roles and responsibilities?

A: Currently, the Performance Evaluation process will not change for the State. It is suggested that agencies begin adopting the PD language to supplement existing performance management processes. This helps formalize roles that already exist within the State, and provides standard expectations across agencies.

Q: How does DIS coordinate and communicate live-training courses that are held by the State?

A: Currently, DIS and EPO communicate upcoming training opportunities directly to Agency Directors. DSHR is currently in the process of hiring an InfoSec and Privacy PDP Manager. The PDP Manager will assist in coordinating and communicating future trainings to a greater audience.

Q: Will the PDP artifacts be uploaded to a Learning Management System (LMS)?

A: The State is working on the implementation of an LMS solution. DSHR will determine how the Training Framework will be uploaded once the LMS is implemented.

Q: How does my agency know what training is aligned to a specific PD or competency?

A: The Training Framework illustrates training courses by certification, competency, and PD.

Q: Why are there multiple competencies associated with different PDs?

A: Each position encompasses a unique mix of InfoSec and Privacy domains. Each PD features the associated competencies from each relevant domain for that position.

Q: Will the recommended training courses found in the PDP Training Framework and Career Path Model provide certifications?

A: Several of the recommended training courses will provide attendees with the ability to obtain a certification upon the completion of additional criteria (e.g., final test, maintaining minimum training hours, etc.). Trainings and vouchers provided by DIS and EPO will be accompanied by a certification attempt.

Q: Are there new requirements on training hours?

A: There is no new requirement on minimum training hours, however, it is a best practice to maintain continuing education (CED) hours. Most certifications in the Training Framework mandate a minimum number of annual CEDs to maintain the certification.

Q: Can certifications obtained by employees (or prospective employees) be verified?

A: Most certifications listed in the Training Framework are nationally accredited and can be verified online. Please visit the accrediting organization to verify the current status of certifications being presented by prospective candidates or current State employees.

Q: Are there any current healthcare related trainings?

A: DIS has procured a number of healthcare and Health Insurance Portability and Accountability Act (HIPAA) related trainings. DIS is working to procure more HIPAA training courses.

Q: Whom should I contact if I have further questions?

A: For additional questions not covered in this document, please contact the InfoSec and Privacy PDP Program Manager or your HR Consultant at (803) 896-5300.