FITSI Job Task Analysis Report 2017

A Job Task
Analysis of the
FITSP-Auditor,
FITSP-Designer,
FITSP-Manager
and FITSP-Operator
Certifications

Version 1.0

Published 8/8/2017

Copyright 2017 FITSI

This page is left intentionally blank

TABLE OF CONTENTS

1. Overview

This report describes the Job Task Analysis (JTA) study for the following Federal IT Security Institute certifications: FITSP-Auditor (FITSP-A), FITSP-Designer (FITSP-D), FITSP-Manager (FITSP-M) and FITSP-Operator (FITSP-O). Each certification examination is designed to assess a candidate's knowledge base and skill sets related to the US Federal Government IT standards put forth by the National Institute of Standards and Technology (NIST). NIST develops standards that are in compliance with the Federal Information Security Management Act (FISMA) passed by Congress in 2002 and updated in 2014 by the Federal Information Security Moderation Act (FISMA 2014). This JTA was conducted in-house by the Federal IT Security Institute (FITSI).

In March of 2006 NIST published Federal Information Processing Standard 200 (FIPS 200) entitled "Minimum Security Requirements for Federal Information and Information Systems." FIPS 200 outlines all the procedures that federal information security practitioners must follow to protect and defend Federal information systems. Noncompliance with these tasks in this standard is a violation of federal law.

FITSI used this mandate to create certification examinations that test the knowledge, skills, and abilities of federal information security practitioners bound by these NIST specifications.

A complete list of specifications for minimum security requirements:

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management (CM): Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response (IR): Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance (MA): Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP): Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Physical and Environmental Protection (PE): Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Program Management (PM): Organizations must ensure that processes and controls are compatible and consistent with an organization's information security program.

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition (SA): Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communications Protection (SC): Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity (SI): Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

The JTA survey posed questions related to each of the above security requirements. The questions were kept general enough to ensure that respondents from any of the four roles: Auditor, Designer, Manager or Operator could answer them.

The results of this JTA will form the basis of the next version of the FITSP certification (version 2.0).

2. Determining Questions and Distribution

The purpose of this survey was to determine the distribution of questions within the certification examination by surveying professionals currently employed in the field. In this way, a passing exam score would correlate with adequate knowledge of the job duties

3. The Study Design

The JTA was carried out via an online survey that was active from March 15th, 2016 – May 31st, 2016. FITSI sent the survey link to 1317 members. 294 respondents completed all or part of the survey. Given the response rate, we can have 95% confidence that the sample is an accurate representation of the population.

The survey consisted of 21 questions. The first two questions allowed the respondent to identify primary job Role (Manager, Auditor, Designer or Operator) and to indicate the length of time in that role. The breakdown of role among survey respondents matched well with the role distribution of the current Certified and Associate FITSI population.

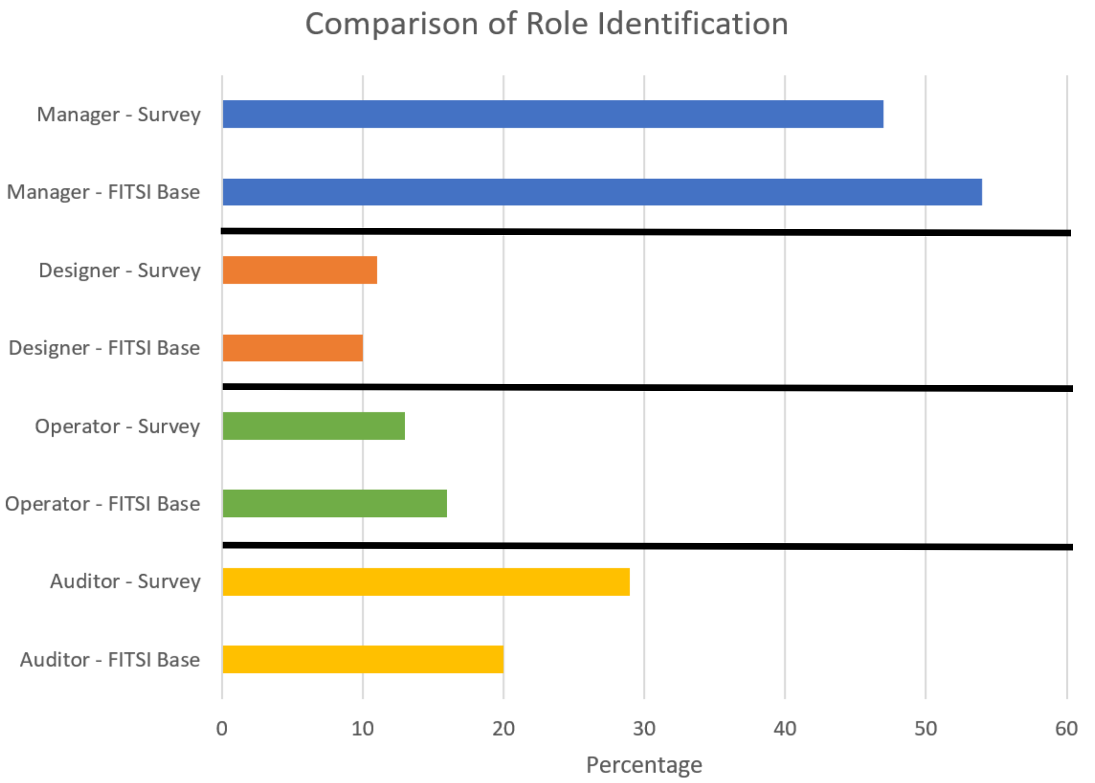


Figure 1: Breakdown of identified Role in the survey

Role	Survey Response %	Survey Response Count	Membership %	Membership Count
Manager	47%	138	54%	710
Designer	11%	32	10%	132
Operator	13%	38	16%	208
Auditor	29%	86	20%	264
Total		294		1317

Table 1: Distribution of identified Role in survey versus identified Role of FITSI Membership

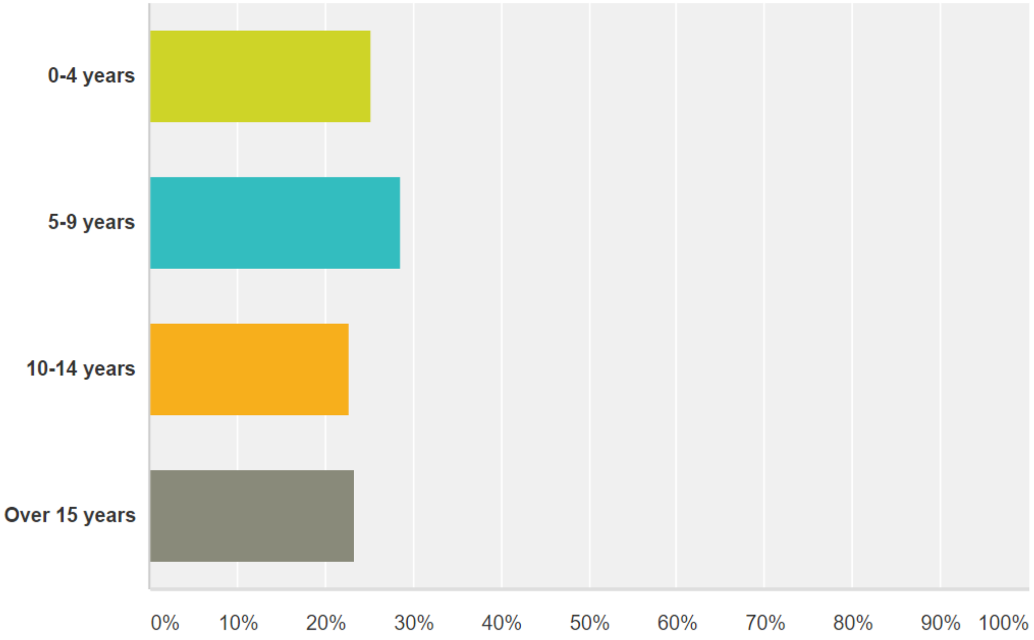


Figure 2: Experience of survey respondents in years for all roles.

The survey shows that the employed respondents were in the current role for a sufficient period and the respondent's distribution was even across the population. This length of time performing duties specific to the identified role ensures survey responses possess real world work experiences.

The next 18 questions dealt with how often the respondent referenced the following resources given a particular task.

The FITSI Job Task Analysis survey uses the following seven resources types:
1. **NIST Special Publications** - These resources focus on the full range of NIST 800 series Special Publications.
Examples: NIST SP 800-37, SP 800-53, SP 800-18, etc.

2. **NIST Federal Information Processing Standards (NIST FIPS**) - This resource focuses on standards such as FIPS 199, FIPS 200, FIPS197 140-2, etc.

3. **NIST Control Families** - This resource focuses on security controls defined in NIST SP 800-53.

4. **Government Laws and Regulations** - This resource focuses on memorandums, circulars, executive orders, and laws that OMB, Congress, and Presidential Directives require.
Examples: FISMA, OMB A-130 Appendix III, HSPD-12, etc.

5. **NIST Risk Management Framework (NIST RMF)** - This resource focuses on NIST RMF in support of system authorization. Example: NIST SP 800-37 Rev 1.

6. **NIST Interagency Reports (NIST IR)** - This resource focuses on reports that concentrate on specific areas.
Examples: IR 7298 Rev2, IR 7756, etc...

7. **Not Applicable (N/A)** - This is to be selected if the respondent doesn't use any of the following resources. Respondents would choose this option when they do not perform that task at work, or they use in-house guidance to carry out that task.

The last question allowed the respondent the option to enter an email address. FITSI collected the email address for a promotional incentive for completing the survey.

The survey questions, as asked, can be seen in Appendix A.

4. Results

The following section summarizes the results of the survey for each of the four FITSP certification roles.

A. FITSP-Auditor

86 respondents indicated the Auditor role when completing the survey. Responses from each question were aggregated to find the percentage that the respondent referred to each of the seven resources given a particular task area. Note that 7% of the time, the respondents referred to none of the provided references. A choice of N/A could be attributed to the respondent not performing that duty or not referencing any document to complete that task. Survey respondents referenced the NIST Special Pubs and NIST Control Families most while performing the specified tasks. NIST IR played little importance in making decisions for this role. The allotment of exam content shall reflect survey results in version 2.0 of the FITSP certification.

Auditor							
	NIST Special Pubs	**NIST FIPS**	**NIST Control Families**	**Laws and Regulations**	**NIST RMF**	**NIST IR**	**N/A**
Percent times Selected	30	6	29	14	12	2	7
Normalized Percent (excludes N/A)	32	7	31	15	13	2	

Table 2: Survey results for Auditor Role

B. FITSP-Designer

32 respondents indicated the Designer role when completing the survey. Responses from each question were aggregated to find the percentage that the respondent referred to each of the seven resources given a particular task area. Note that 8% of the time, the respondents referred to none of the provided references. A choice of N/A could be attributed to the respondent not performing that duty or not referencing any document to complete that task. FITSI normalized the results across the six resources. Survey respondents referenced the NIST Special Pubs and NIST Control Families most while performing the specified tasks. NIST IR played little importance in making decisions for this role. The allotment of exam content shall reflect survey results in version 2.0 of the FITSP certification.

Designer							
	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Percent times Selected	22	11	23	19	15	2	8
Normalized Percent (excludes N/A)	24	12	25	21	16	2	

Table 3: Survey results for Designer Role

C. FITSP-Manager

138 respondents indicated the Manager role when completing the survey. Responses from each question were aggregated to find the percentage that the respondent referred to each of the seven resources given a particular task area. Note that 6% of the time, the respondents referred to none of the provided references. A choice of N/A could be attributed to the respondent not performing that duty or not referencing any document to complete that task. FITSI normalized the results across the six resources. Survey respondents referenced the NIST Special Pubs and NIST Control Families most while performing the specified tasks. NIST IR played little importance in making decisions for this role. The allotment of exam content shall reflect survey results in version 2.0 of the FITSP certification.

Manager							
	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Percent times Selected	25	10	23	16	17	3	6
Normalized Percent (excludes N/A)	27	11	24	17	18	3	

Table 4: Survey results for Manager Role

D. FITSP-Operator

38 respondents indicated the Operator role when completing the survey. Responses from each question were aggregated to find the percentage that the respondent referred to each of the seven resources given a particular task area. Note that 16% of the time, the respondents referred to none of the provided references. A choice of N/A could be attributed to the respondent not performing that duty or not referencing any document to complete that task. FITSI normalized the results across the six resources. Survey respondents referenced the NIST Special Pubs and NIST Control Families most while performing the specified tasks. NIST IR played little importance in making decisions for this role. The allotment of exam content shall reflect survey results in version 2.0 of the FITSP certification.

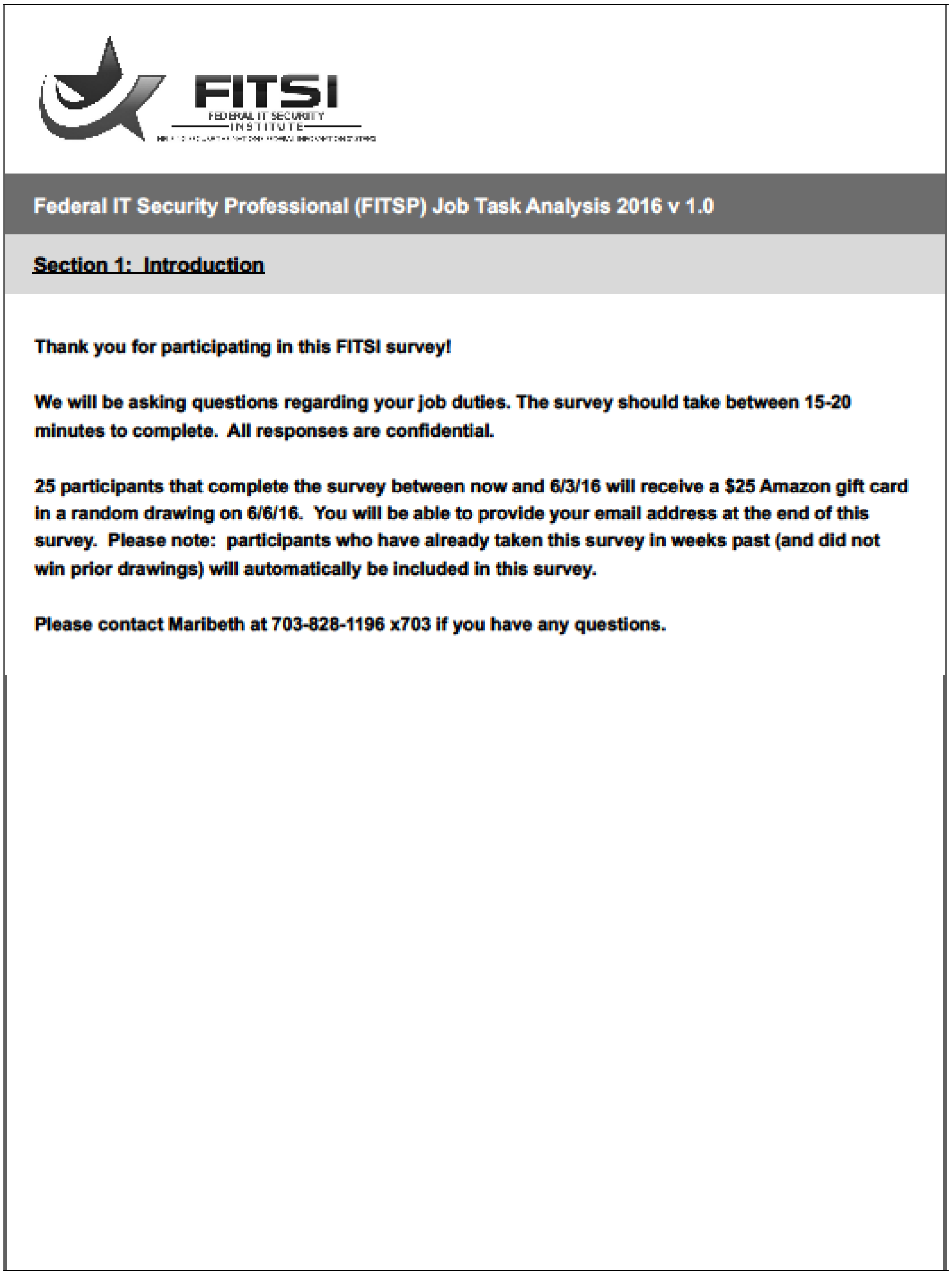
Operator							
	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Percent times Selected	29	15	21	8	9	2	16
Normalized Percent (excludes N/A)	34	18	25	10	11	2	

Table 5: Survey results for Operator Role

5. Summary

The results of the JTA were encouraging. The respondent role distribution was a good reflection of the FITSI member database distribution. Survey results indicated the respondents rely heavily on guidance from NIST Special Pubs and NIST Control Families. The data provided guidance in determining the source and distribution of the examination content for the FITSP 2.0 certification exams.

Appendix A – FITSP Job Task Analysis Survey



Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

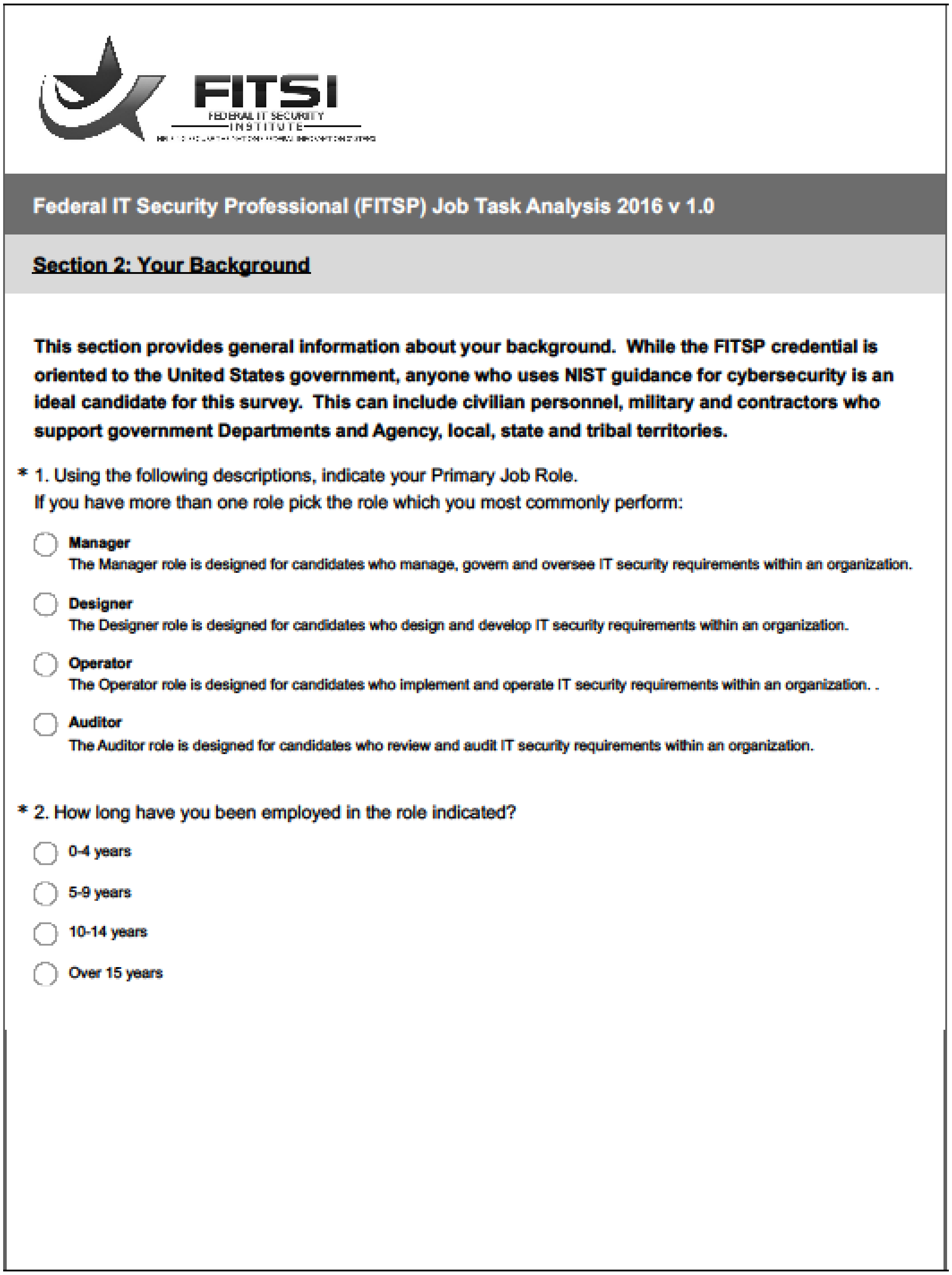
Section 1: Introduction

Thank you for participating in this FITSI survey!

We will be asking questions regarding your job duties. The survey should take between 15-20 minutes to complete. All responses are confidential.

25 participants that complete the survey between now and 6/3/16 will receive a $25 Amazon gift card in a random drawing on 6/6/16. You will be able to provide your email address at the end of this survey. Please note: participants who have already taken this survey in weeks past (and did not win prior drawings) will automatically be included in this survey.

Please contact Maribeth at 703-828-1196 x703 if you have any questions.



Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 2: Your Background

This section provides general information about your background. While the FITSP credential is oriented to the United States government, anyone who uses NIST guidance for cybersecurity is an ideal candidate for this survey. This can include civilian personnel, military and contractors who support government Departments and Agency, local, state and tribal territories.

* 1. Using the following descriptions, indicate your Primary Job Role.
If you have more than one role pick the role which you most commonly perform:

○ **Manager**
The Manager role is designed for candidates who manage, govern and oversee IT security requirements within an organization.

○ **Designer**
The Designer role is designed for candidates who design and develop IT security requirements within an organization.

○ **Operator**
The Operator role is designed for candidates who implement and operate IT security requirements within an organization. .

○ **Auditor**
The Auditor role is designed for candidates who review and audit IT security requirements within an organization.

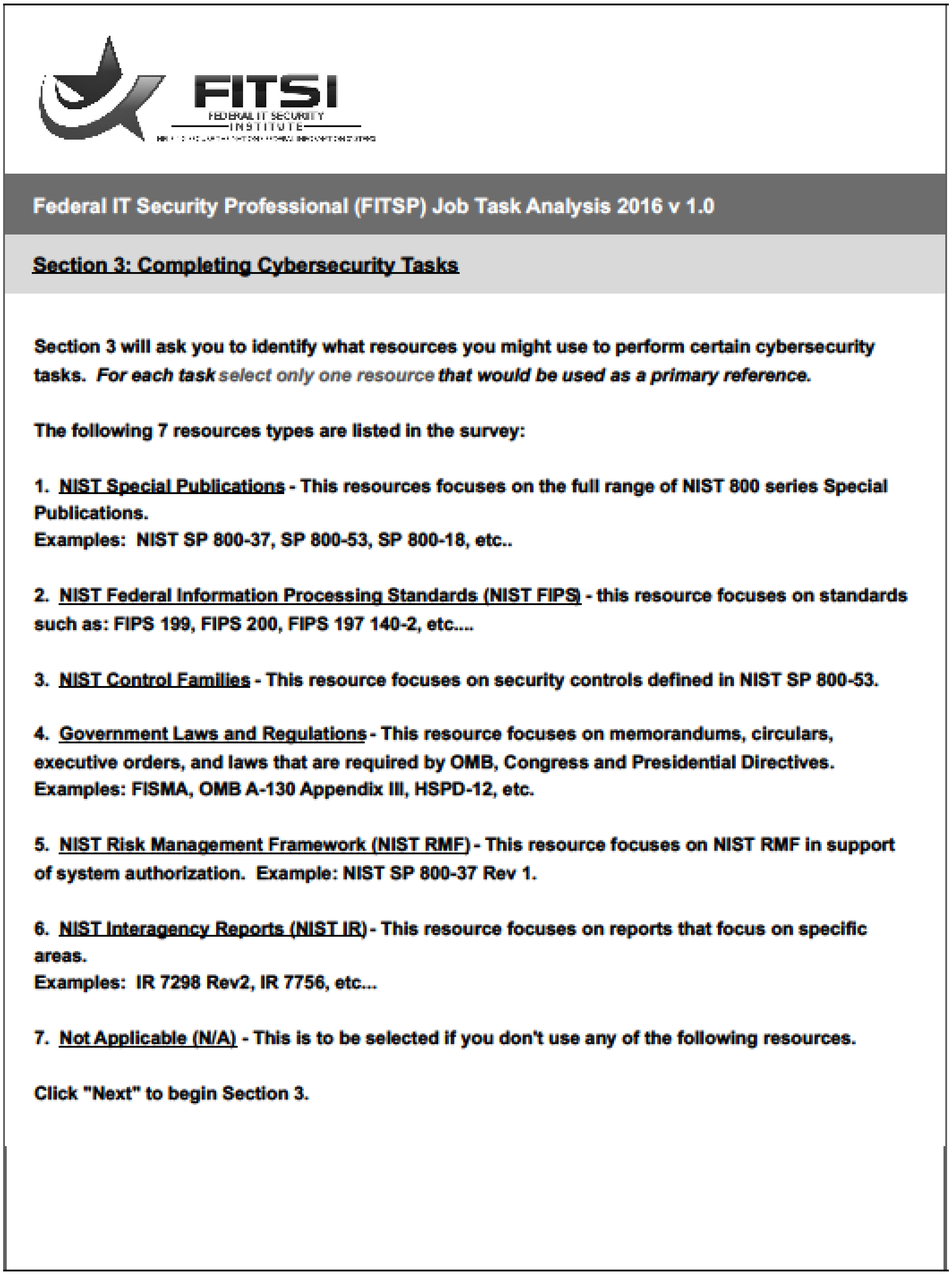
* 2. How long have you been employed in the role indicated?

○ 0-4 years

○ 5-9 years

○ 10-14 years

○ Over 15 years



Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Completing Cybersecurity Tasks

Section 3 will ask you to identify what resources you might use to perform certain cybersecurity tasks. *For each task select only one resource that would be used as a primary reference.*

The following 7 resources types are listed in the survey:

1. NIST Special Publications - This resources focuses on the full range of NIST 800 series Special Publications.
Examples: NIST SP 800-37, SP 800-53, SP 800-18, etc..

2. NIST Federal Information Processing Standards (NIST FIPS) - this resource focuses on standards such as: FIPS 199, FIPS 200, FIPS 197 140-2, etc....

3. NIST Control Families - This resource focuses on security controls defined in NIST SP 800-53.

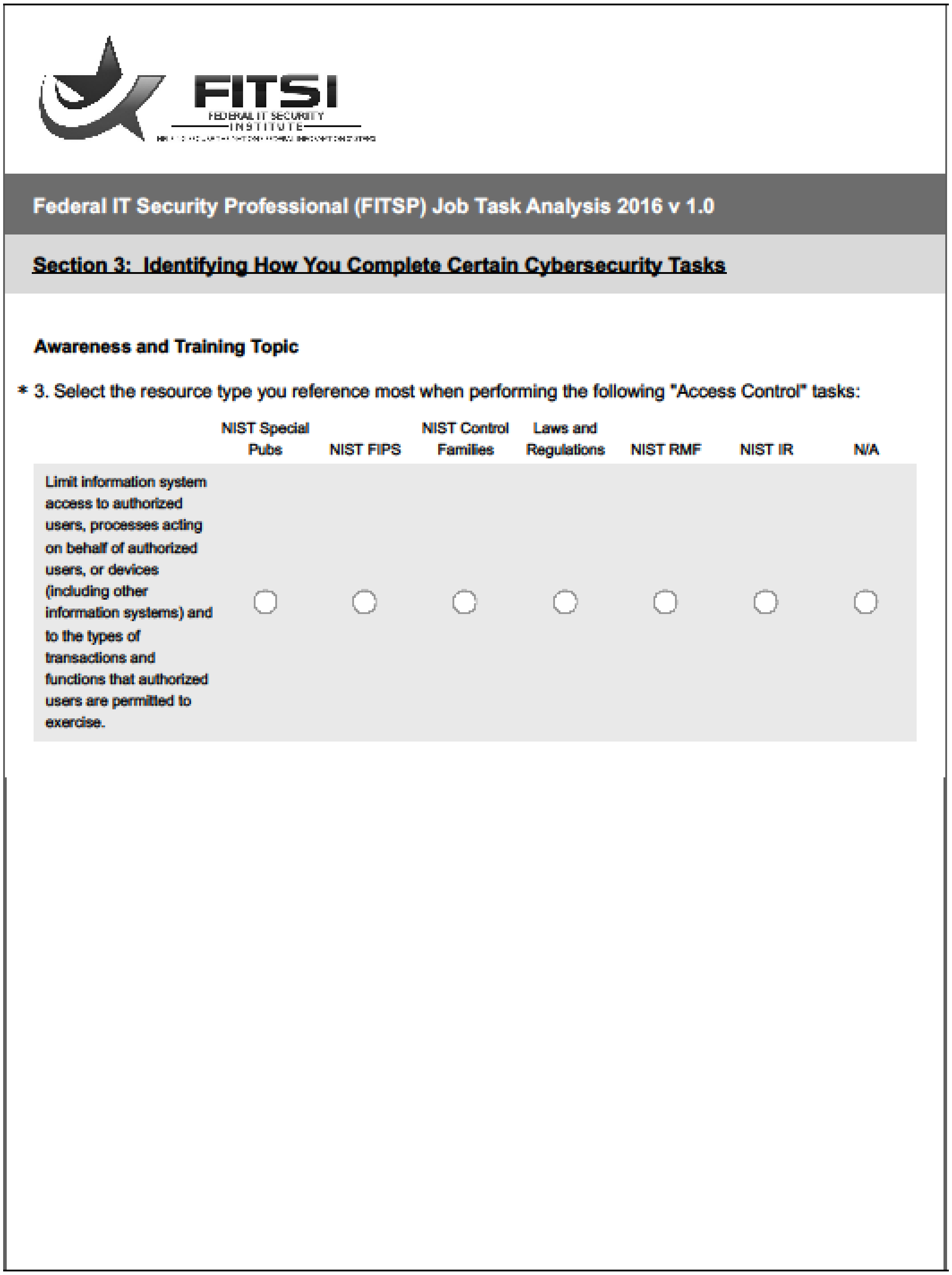
4. Government Laws and Regulations - This resource focuses on memorandums, circulars, executive orders, and laws that are required by OMB, Congress and Presidential Directives.
Examples: FISMA, OMB A-130 Appendix III, HSPD-12, etc.

5. NIST Risk Management Framework (NIST RMF) - This resource focuses on NIST RMF in support of system authorization. Example: NIST SP 800-37 Rev 1.

6. NIST Interagency Reports (NIST IR) - This resource focuses on reports that focus on specific areas.
Examples: IR 7298 Rev2, IR 7756, etc...

7. Not Applicable (N/A) - This is to be selected if you don't use any of the following resources.

Click "Next" to begin Section 3.



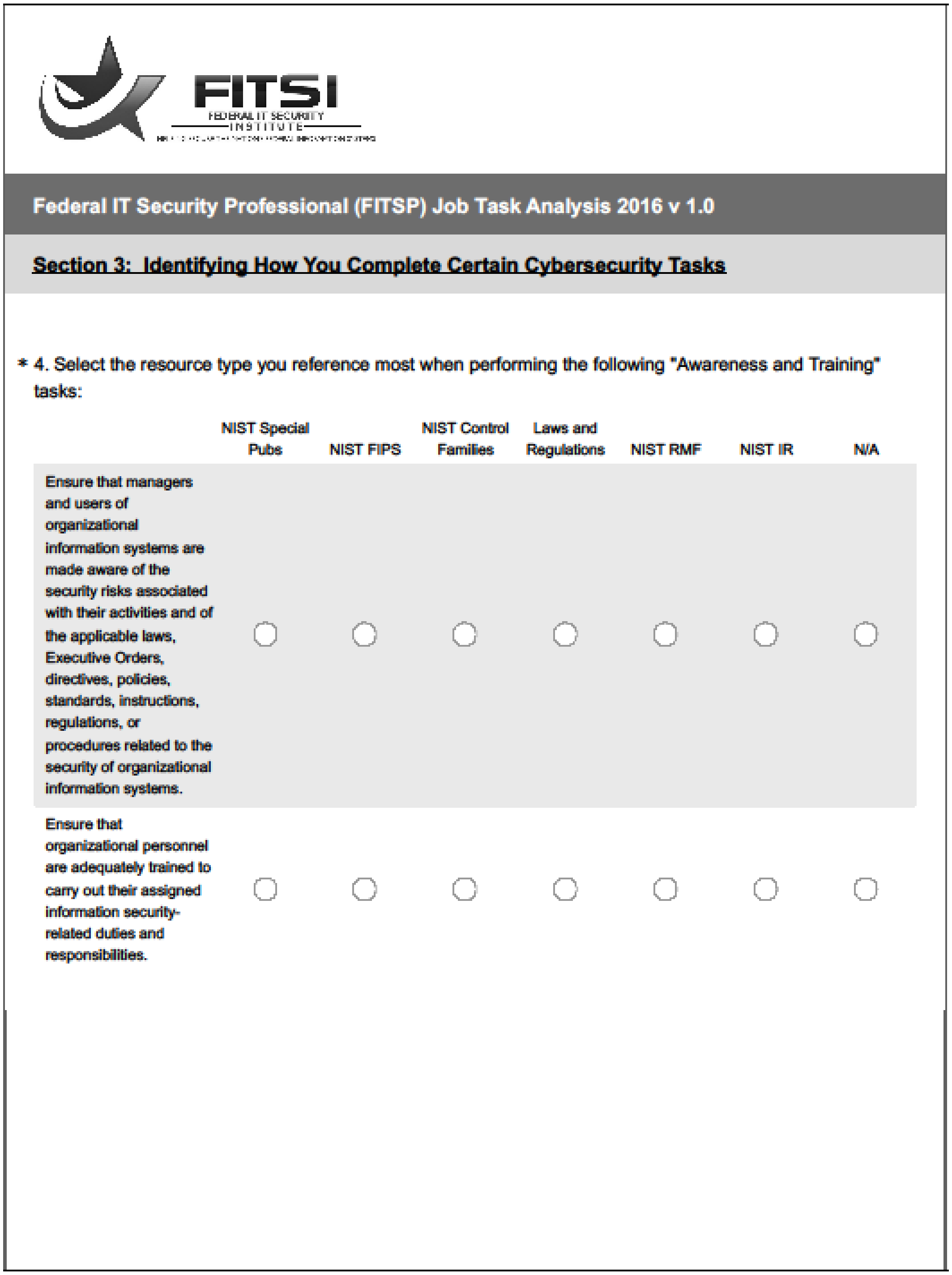
Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

Awareness and Training Topic

* 3. Select the resource type you reference most when performing the following "Access Control" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	○	○	○	○	○	○	○

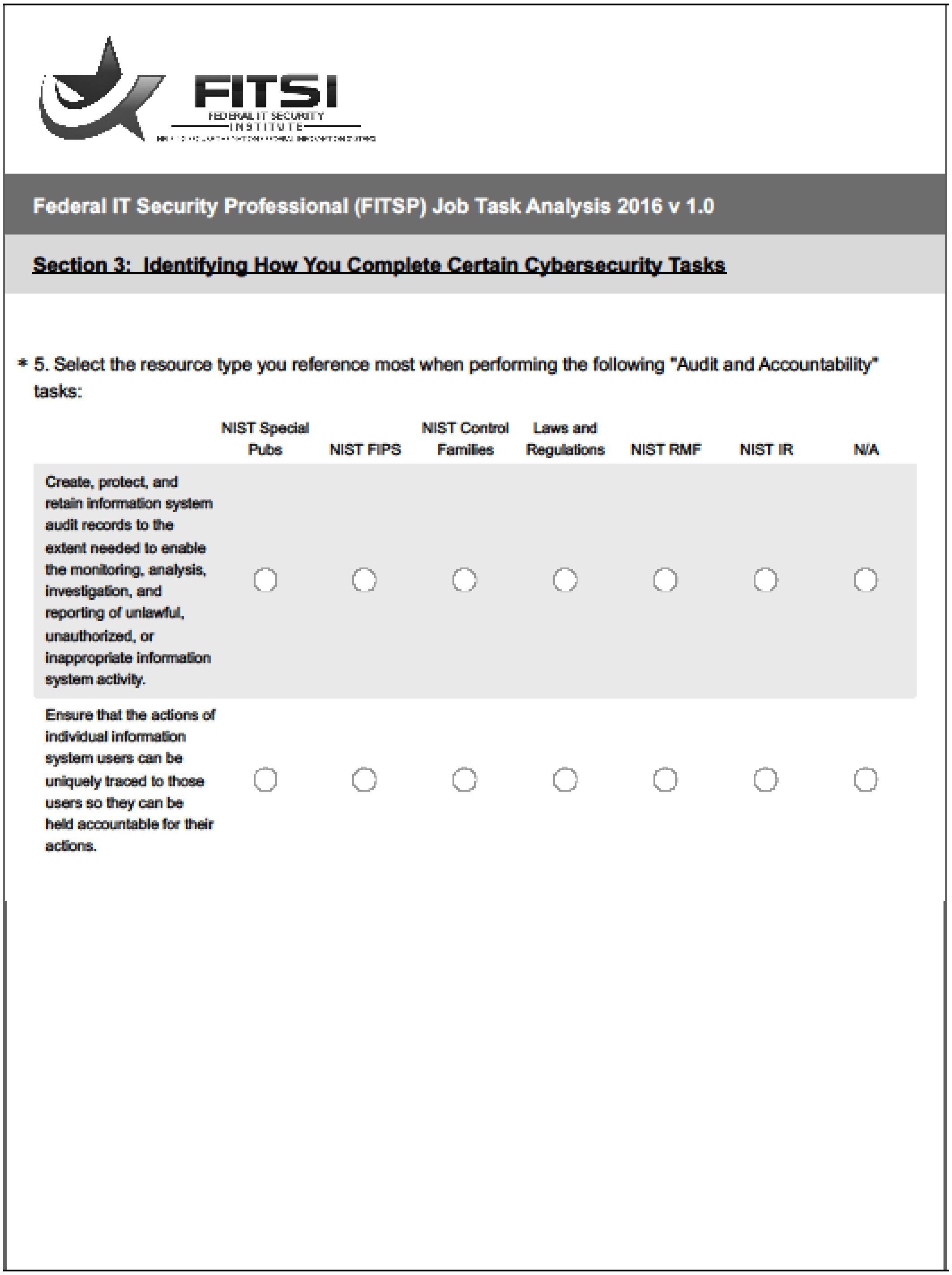


Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 4. Select the resource type you reference most when performing the following "Awareness and Training" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems.	○	○	○	○	○	○	○
Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	○	○	○	○	○	○	○



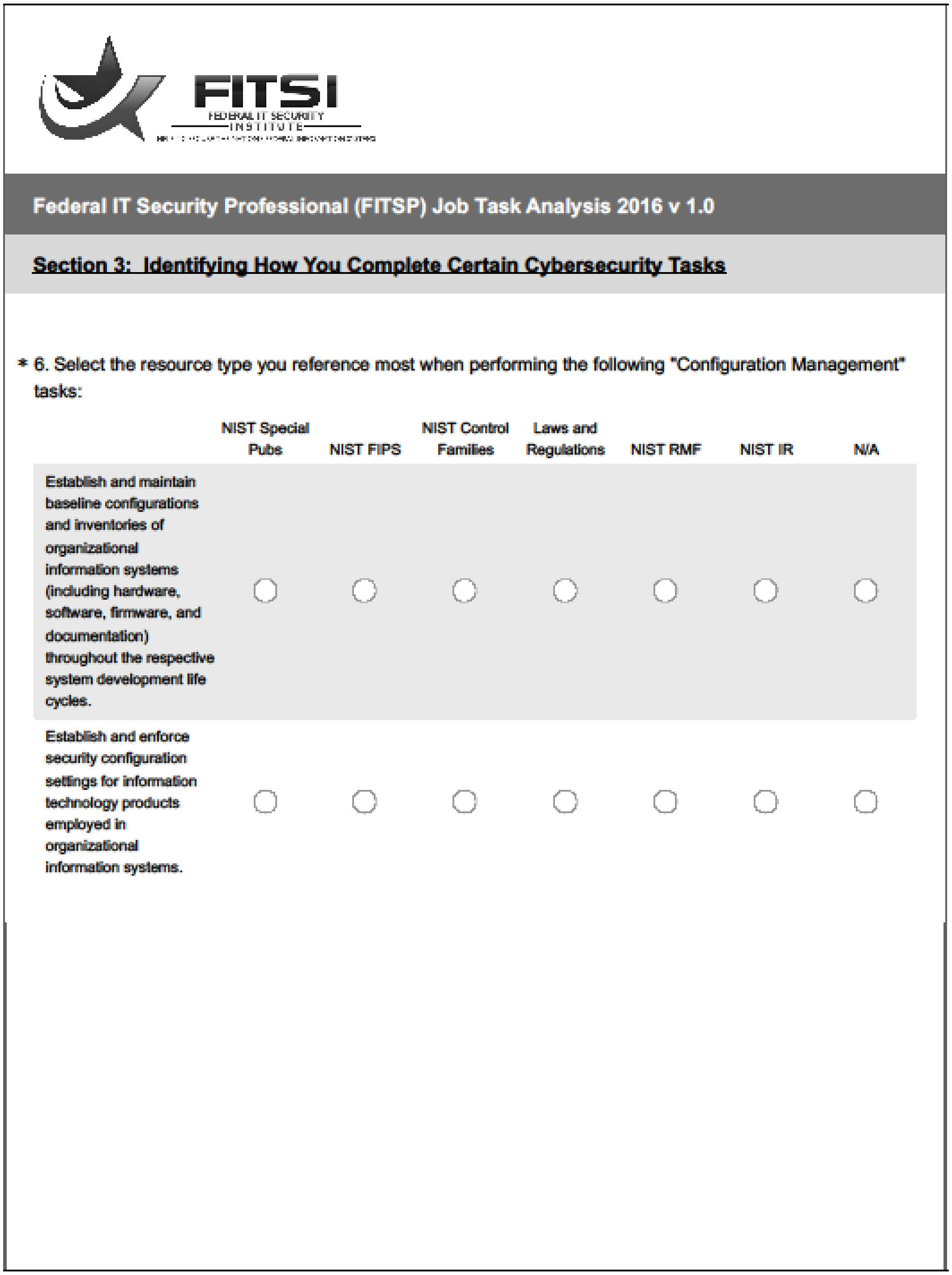
FITSI
FEDERAL IT SECURITY INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 5. Select the resource type you reference most when performing the following "Audit and Accountability" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	○	○	○	○	○	○	○
Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	○	○	○	○	○	○	○



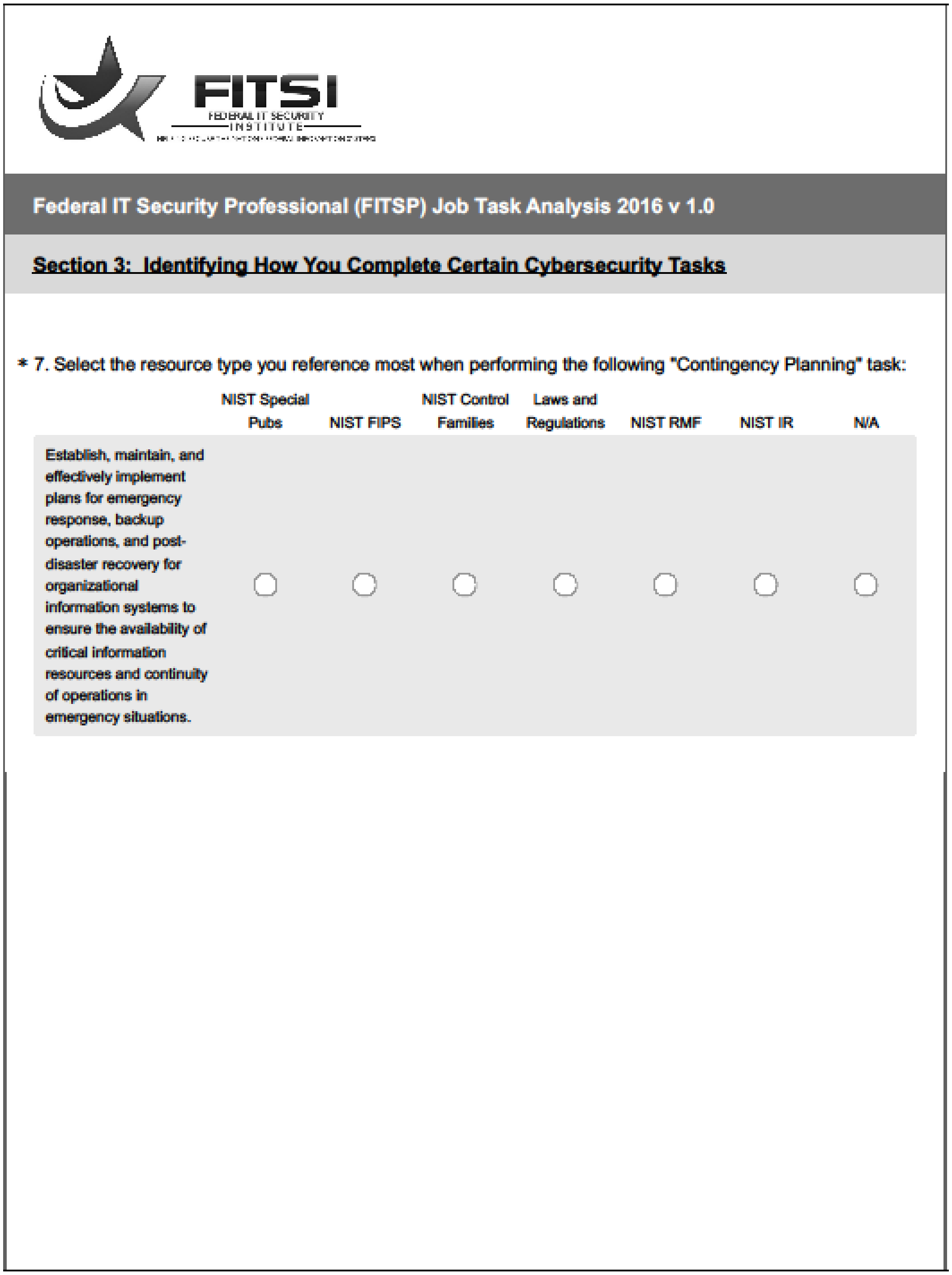
FITSI
FEDERAL IT SECURITY
INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 6. Select the resource type you reference most when performing the following "Configuration Management" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	○	○	○	○	○	○	○
Establish and enforce security configuration settings for information technology products employed in organizational information systems.	○	○	○	○	○	○	○



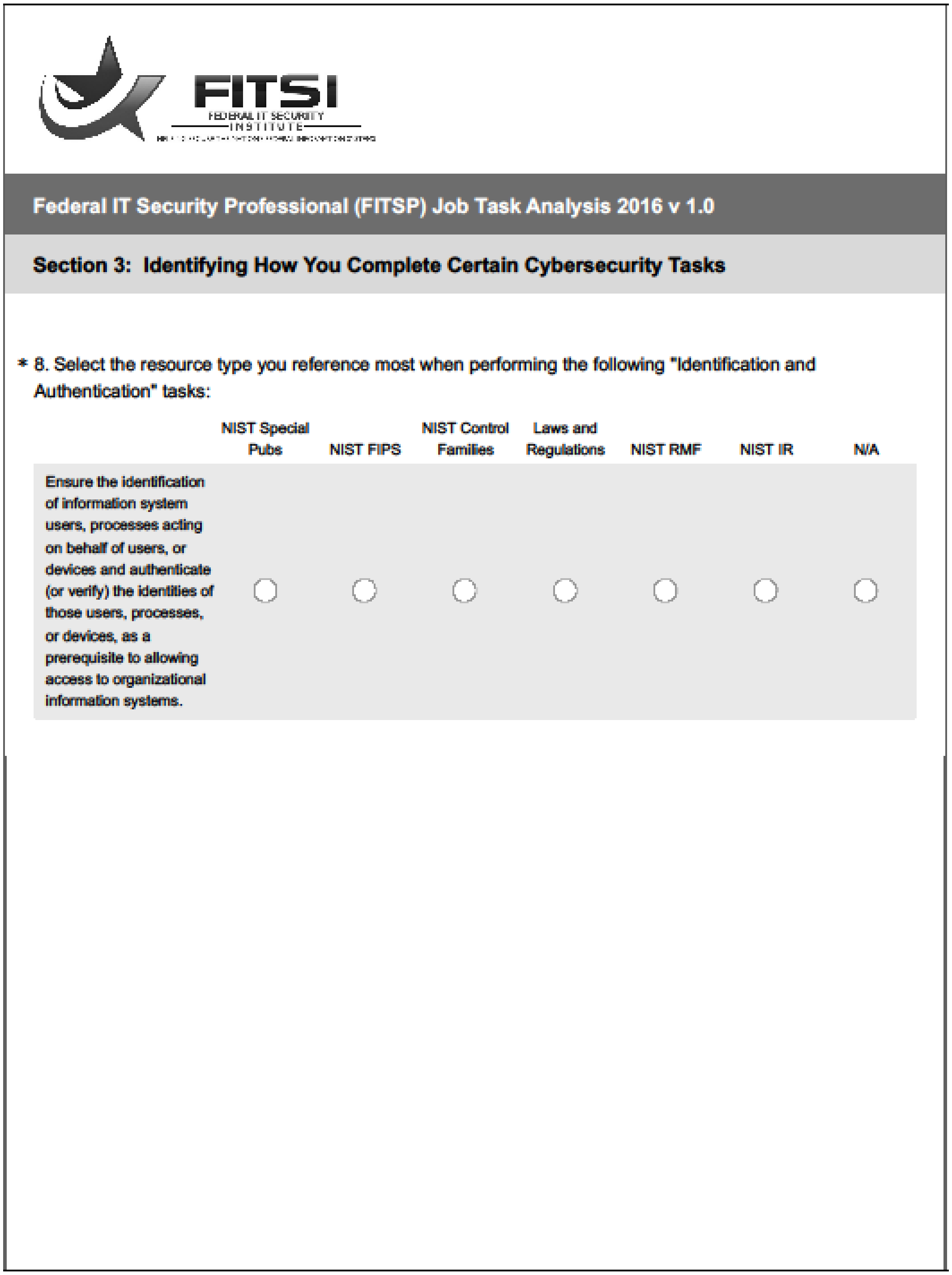
FITSI
FEDERAL IT SECURITY
INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 7. Select the resource type you reference most when performing the following "Contingency Planning" task:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.	○	○	○	○	○	○	○

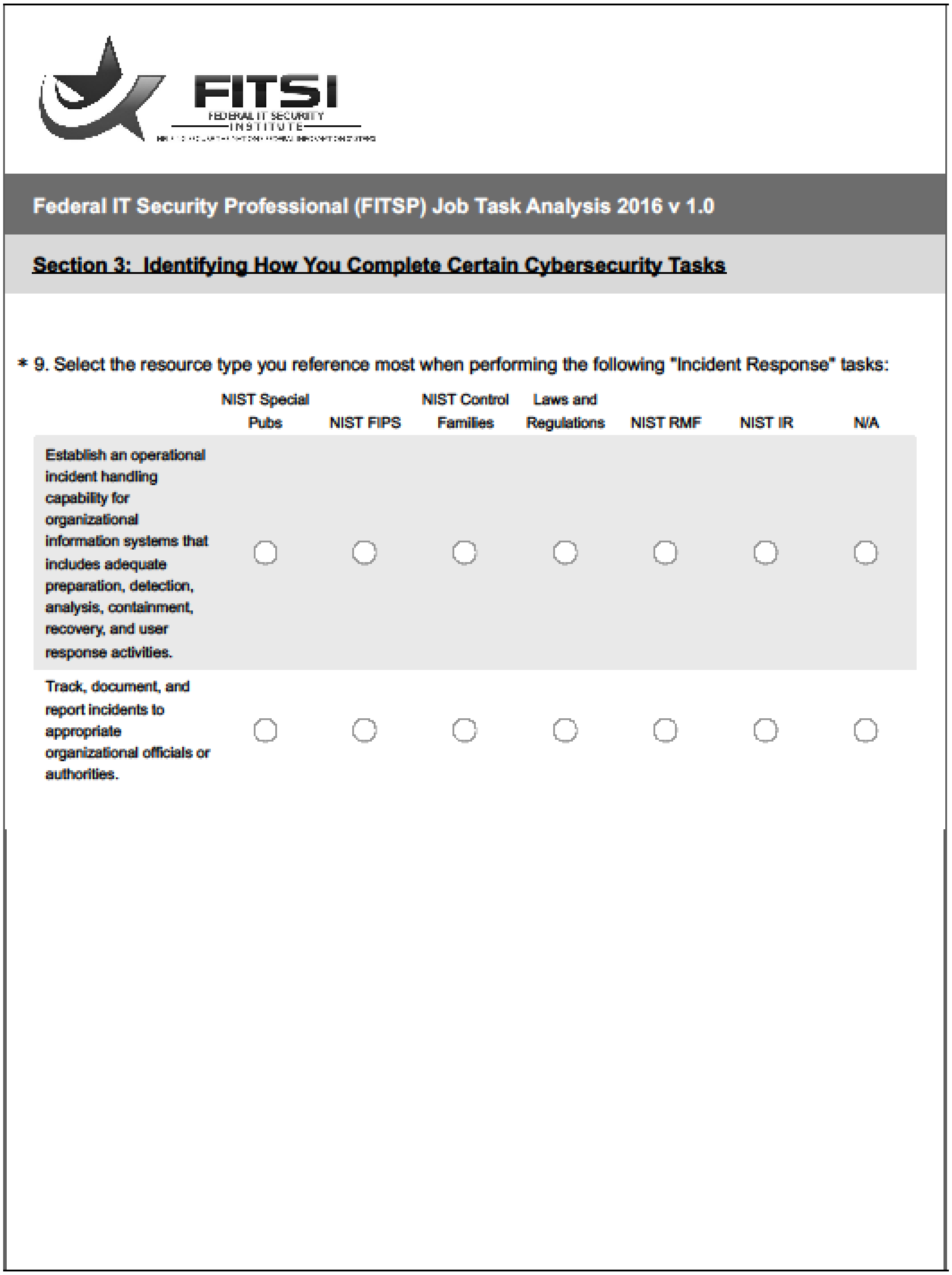


Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 8. Select the resource type you reference most when performing the following "Identification and Authentication" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Ensure the identification of information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	○	○	○	○	○	○	○

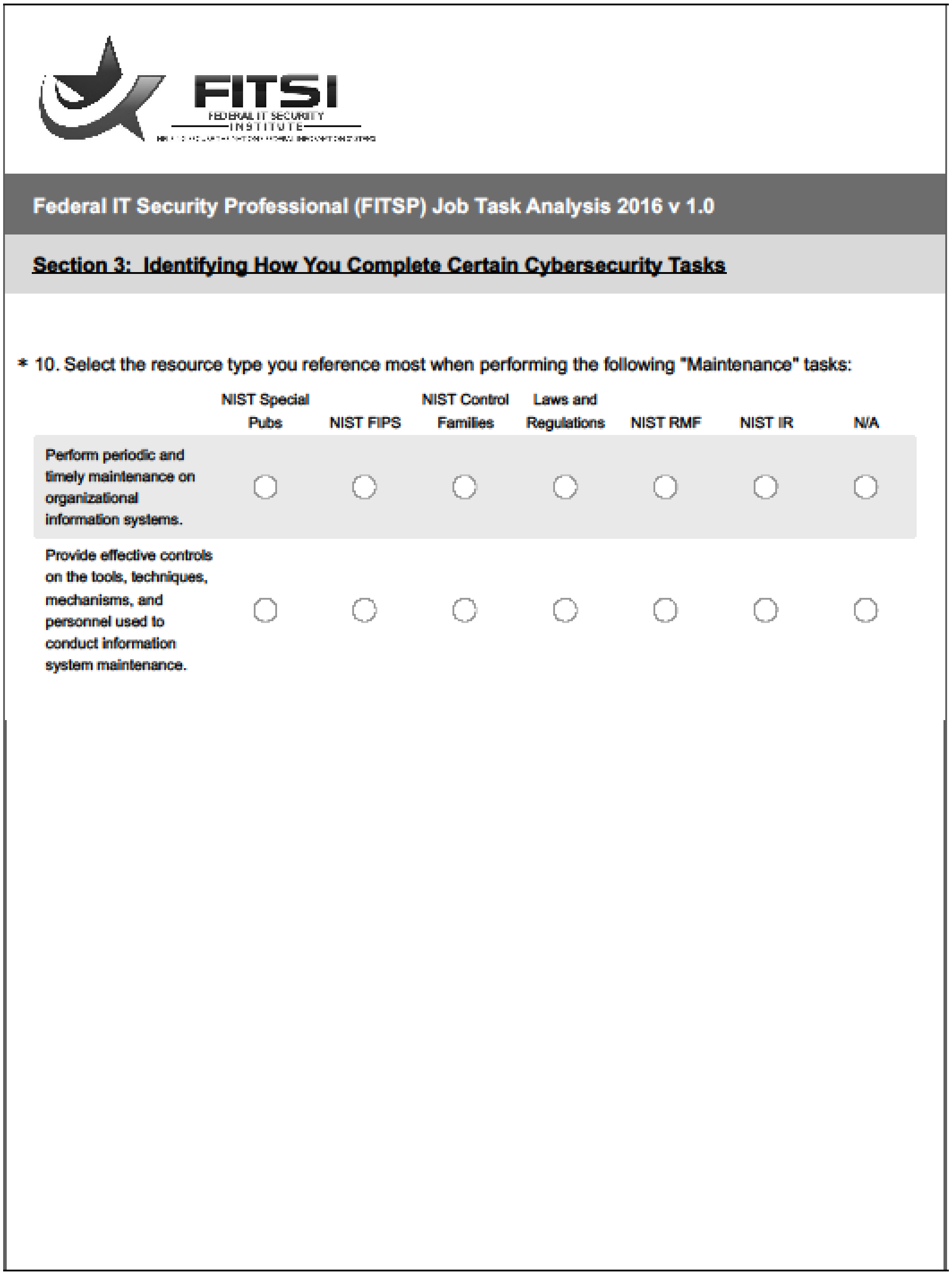


Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 9. Select the resource type you reference most when performing the following "Incident Response" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	○	○	○	○	○	○	○
Track, document, and report incidents to appropriate organizational officials or authorities.	○	○	○	○	○	○	○

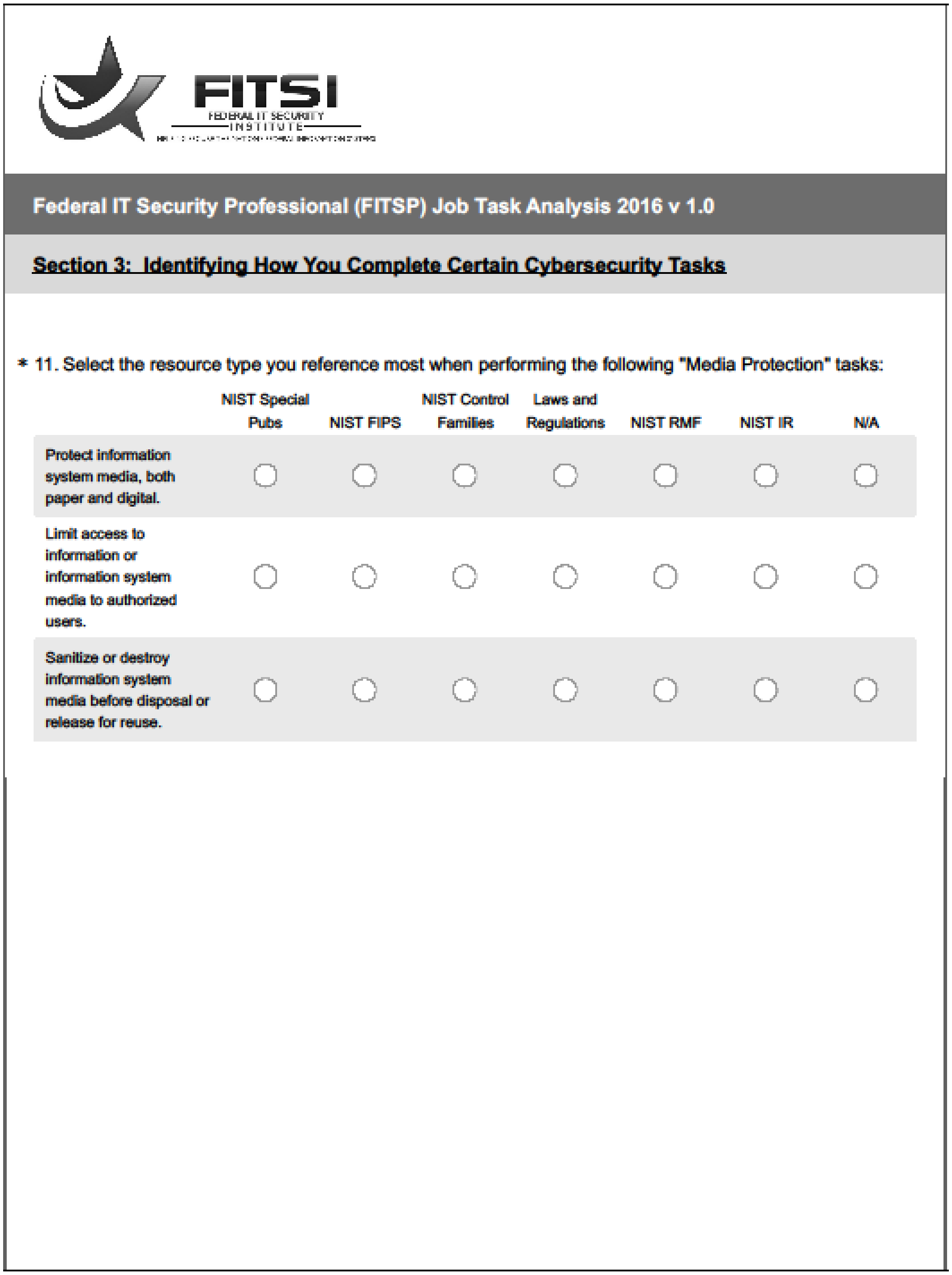


Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 10. Select the resource type you reference most when performing the following "Maintenance" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Perform periodic and timely maintenance on organizational information systems.	○	○	○	○	○	○	○
Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	○	○	○	○	○	○	○

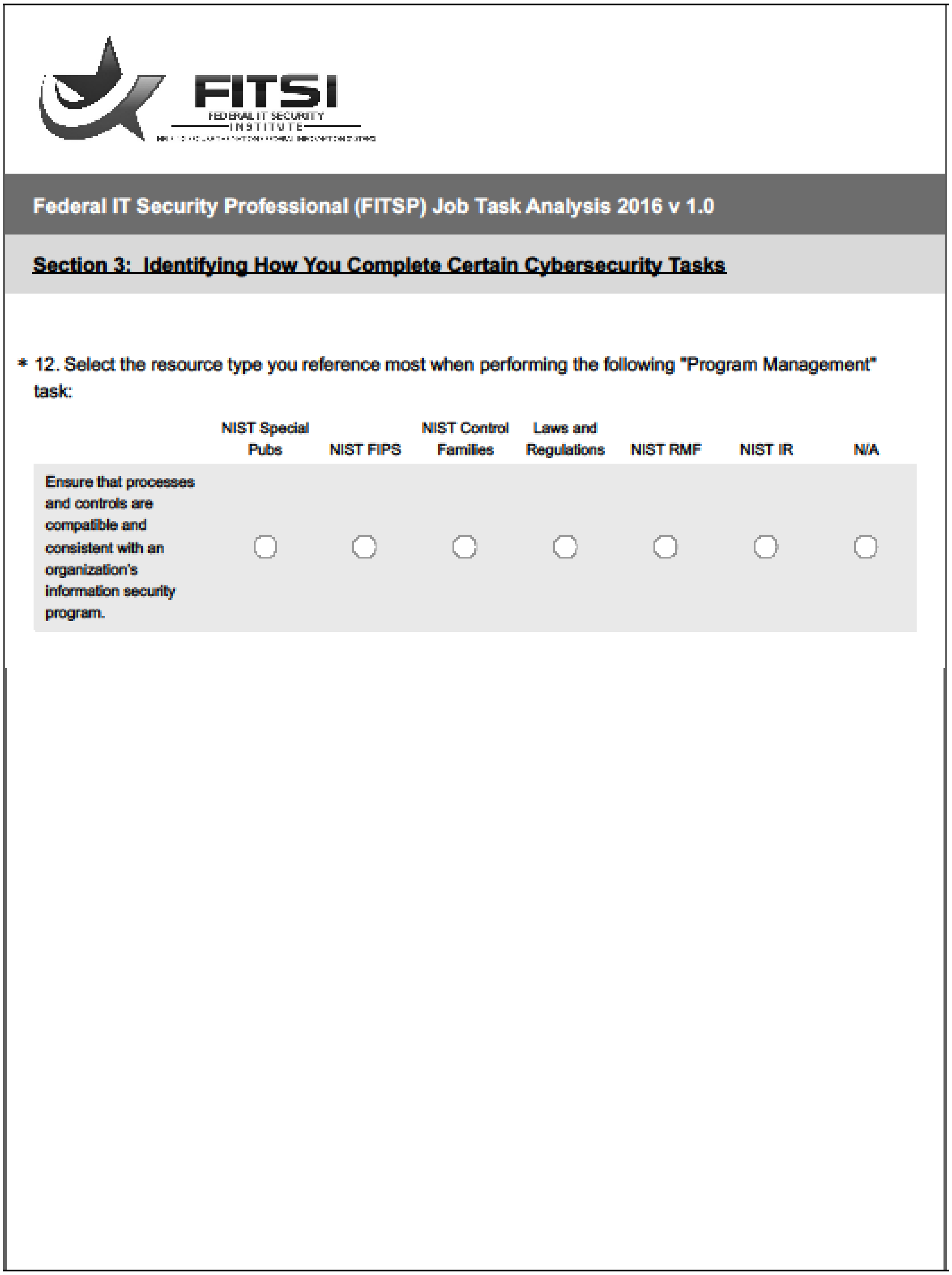


Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 11. Select the resource type you reference most when performing the following "Media Protection" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Protect information system media, both paper and digital.	○	○	○	○	○	○	○
Limit access to information or information system media to authorized users.	○	○	○	○	○	○	○
Sanitize or destroy information system media before disposal or release for reuse.	○	○	○	○	○	○	○



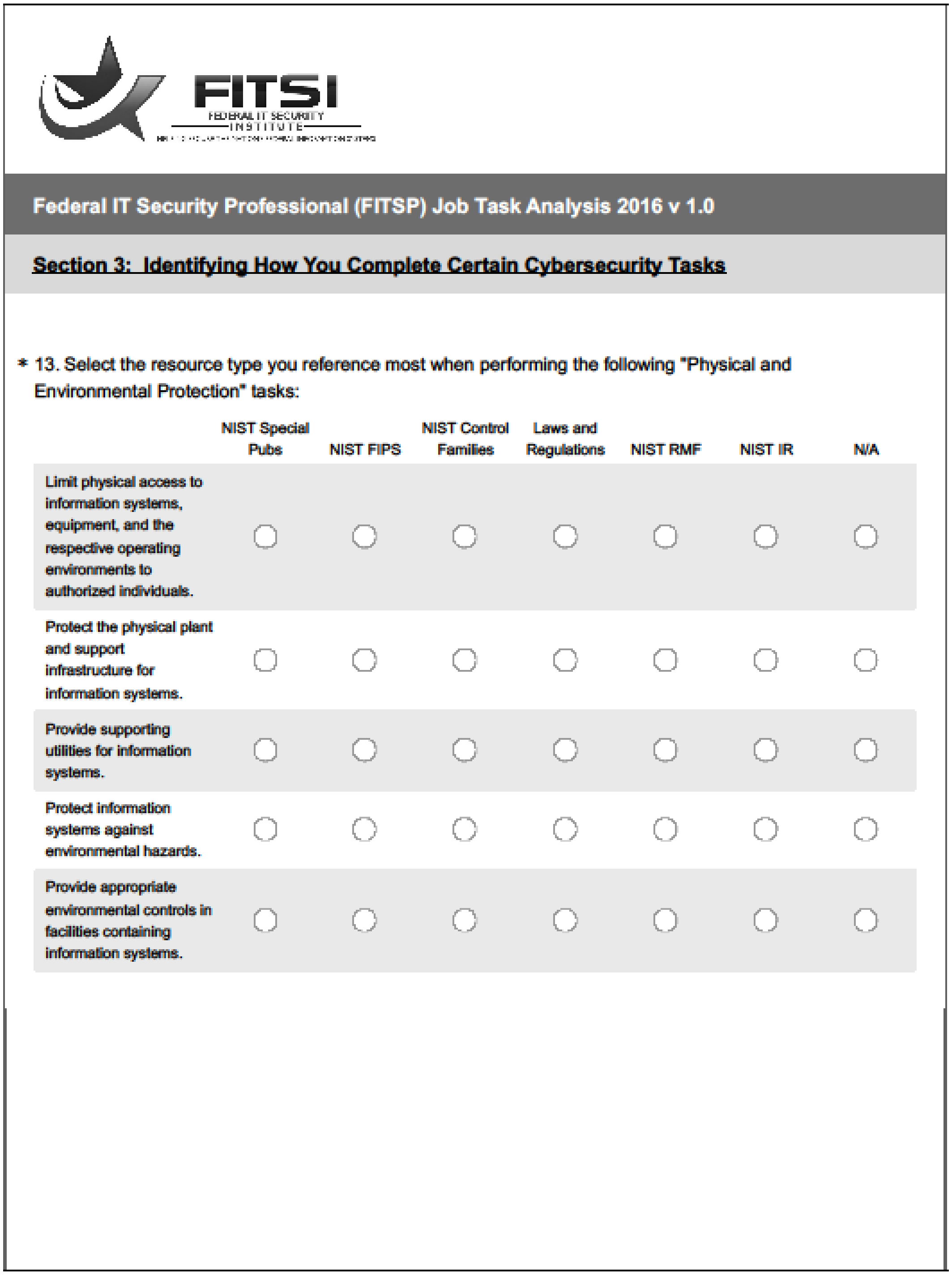
FITSI
FEDERAL IT SECURITY
INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 12. Select the resource type you reference most when performing the following "Program Management" task:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Ensure that processes and controls are compatible and consistent with an organization's information security program.	○	○	○	○	○	○	○



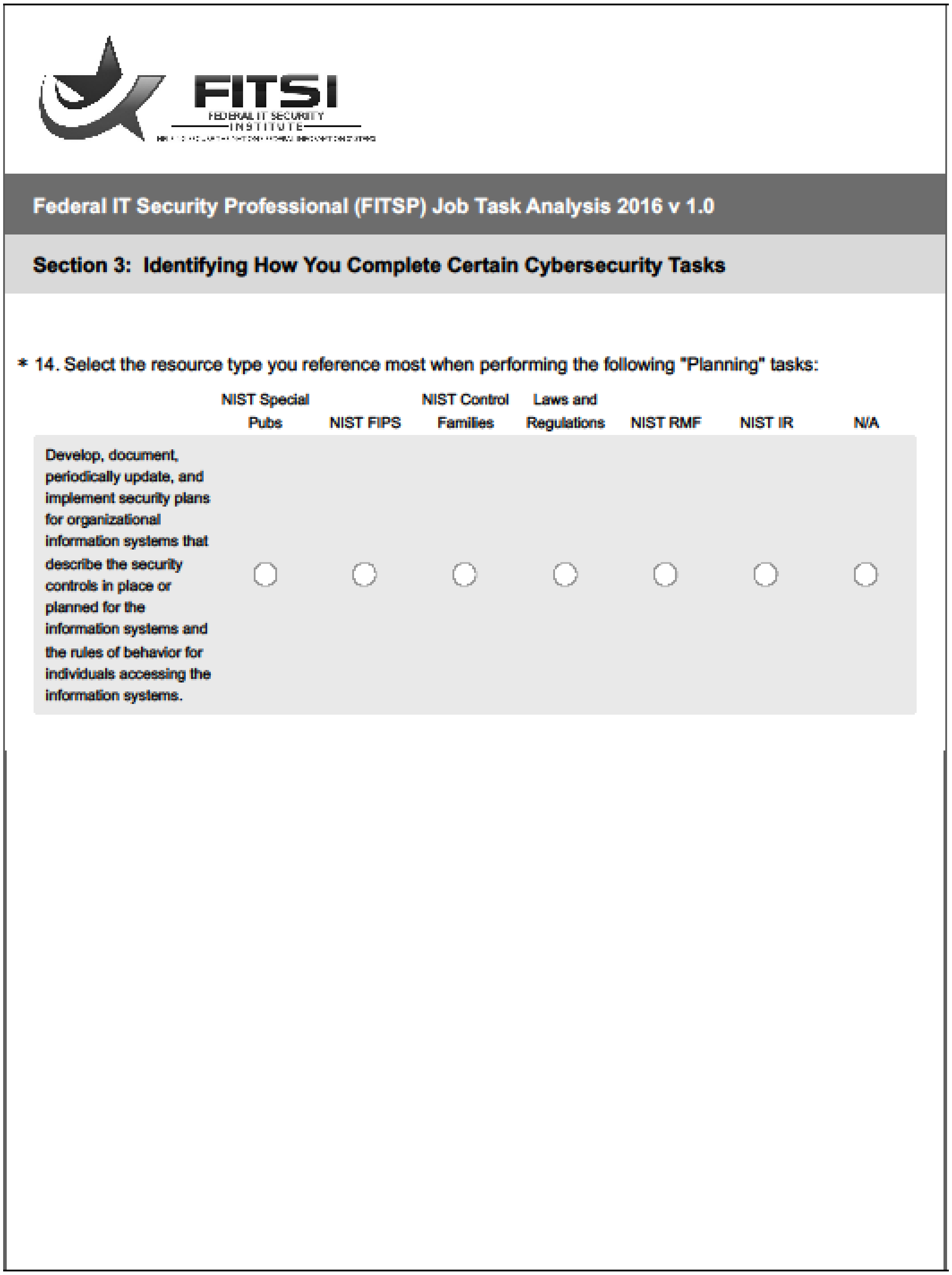
FITSI
FEDERAL IT SECURITY
INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 13. Select the resource type you reference most when performing the following "Physical and Environmental Protection" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.	○	○	○	○	○	○	○
Protect the physical plant and support infrastructure for information systems.	○	○	○	○	○	○	○
Provide supporting utilities for information systems.	○	○	○	○	○	○	○
Protect information systems against environmental hazards.	○	○	○	○	○	○	○
Provide appropriate environmental controls in facilities containing information systems.	○	○	○	○	○	○	○

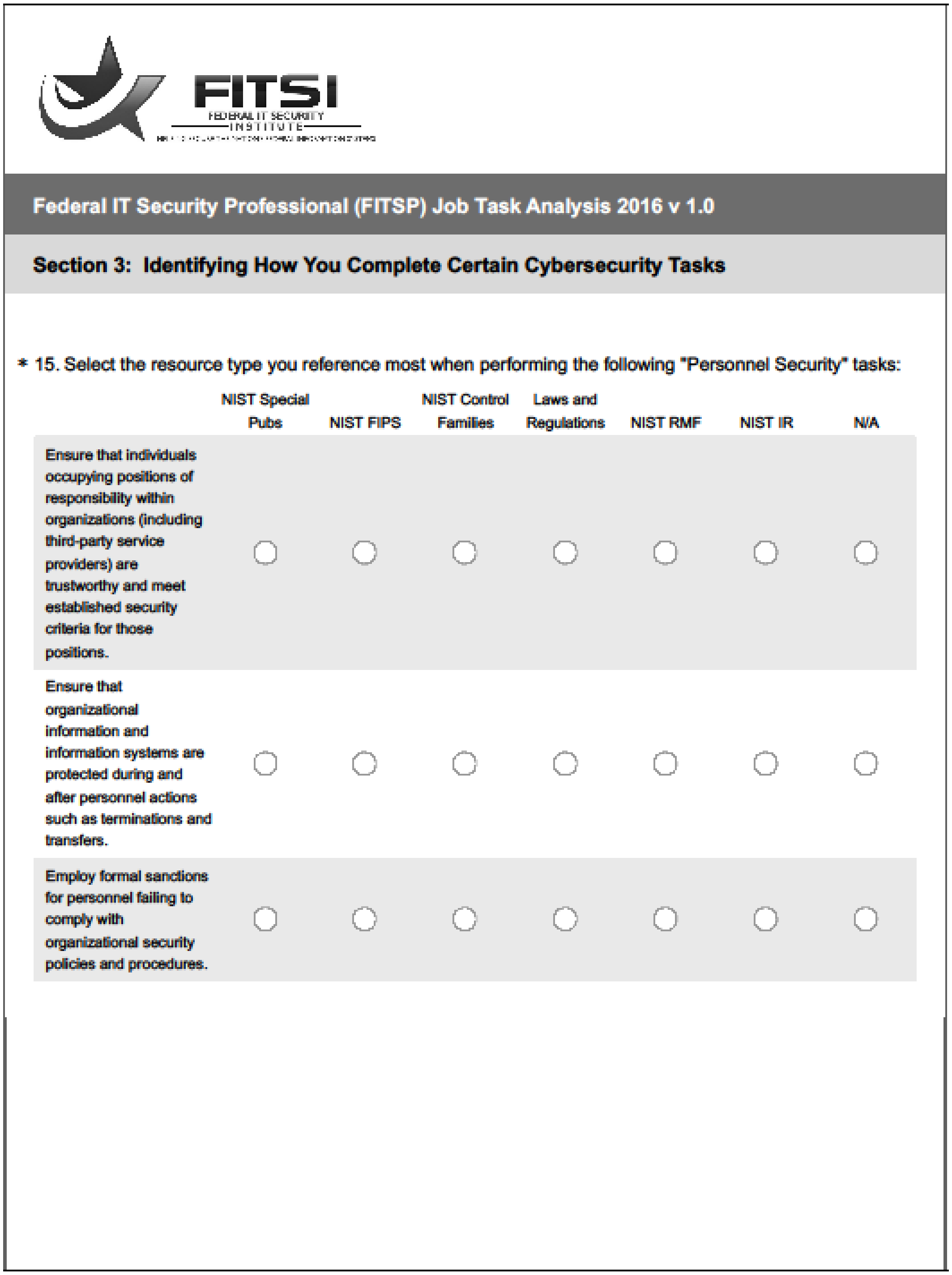


Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 14. Select the resource type you reference most when performing the following "Planning" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.	○	○	○	○	○	○	○



FITSI

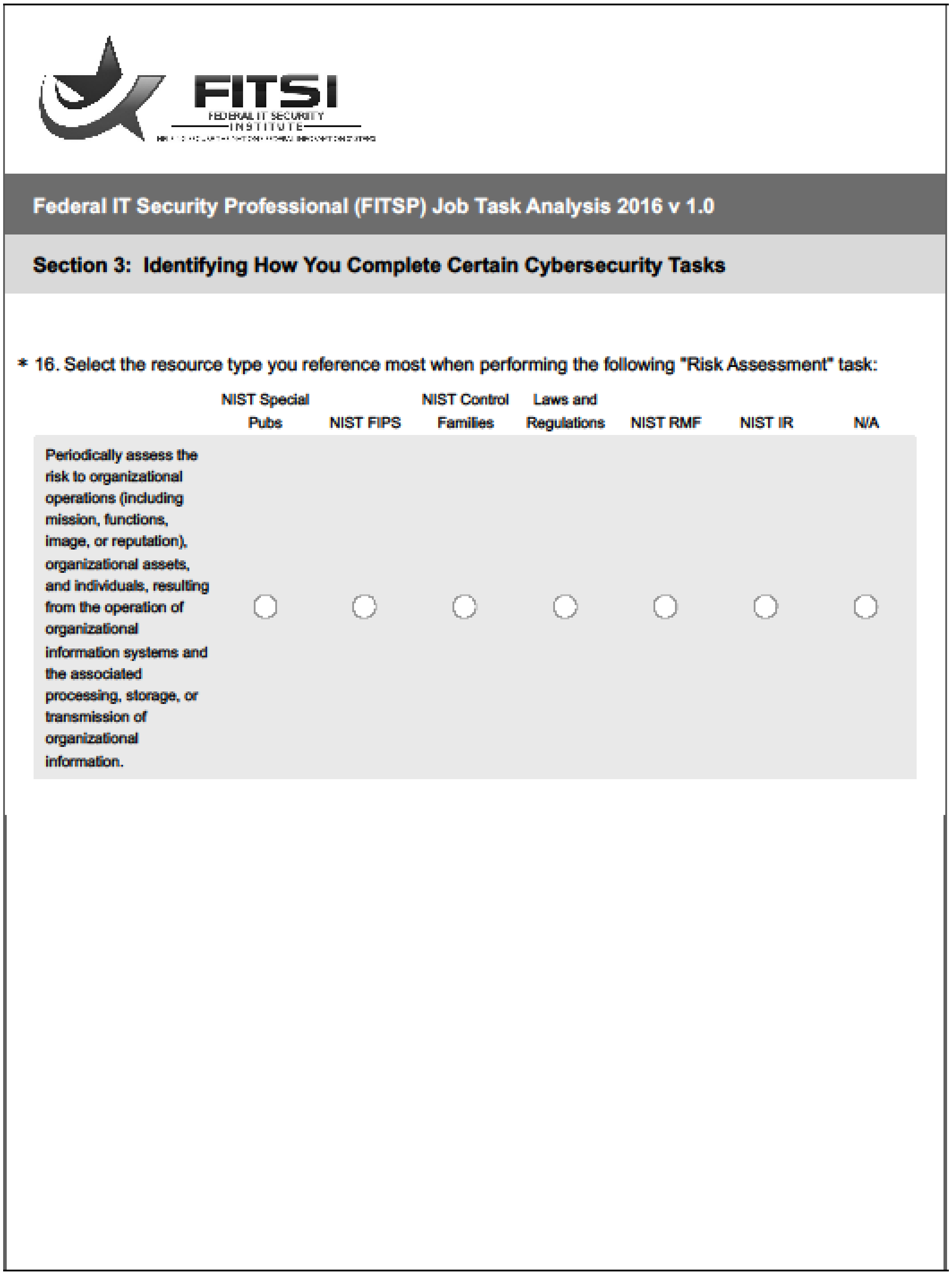
FEDERAL IT SECURITY INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 15. Select the resource type you reference most when performing the following "Personnel Security" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions.	○	○	○	○	○	○	○
Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.	○	○	○	○	○	○	○
Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.	○	○	○	○	○	○	○

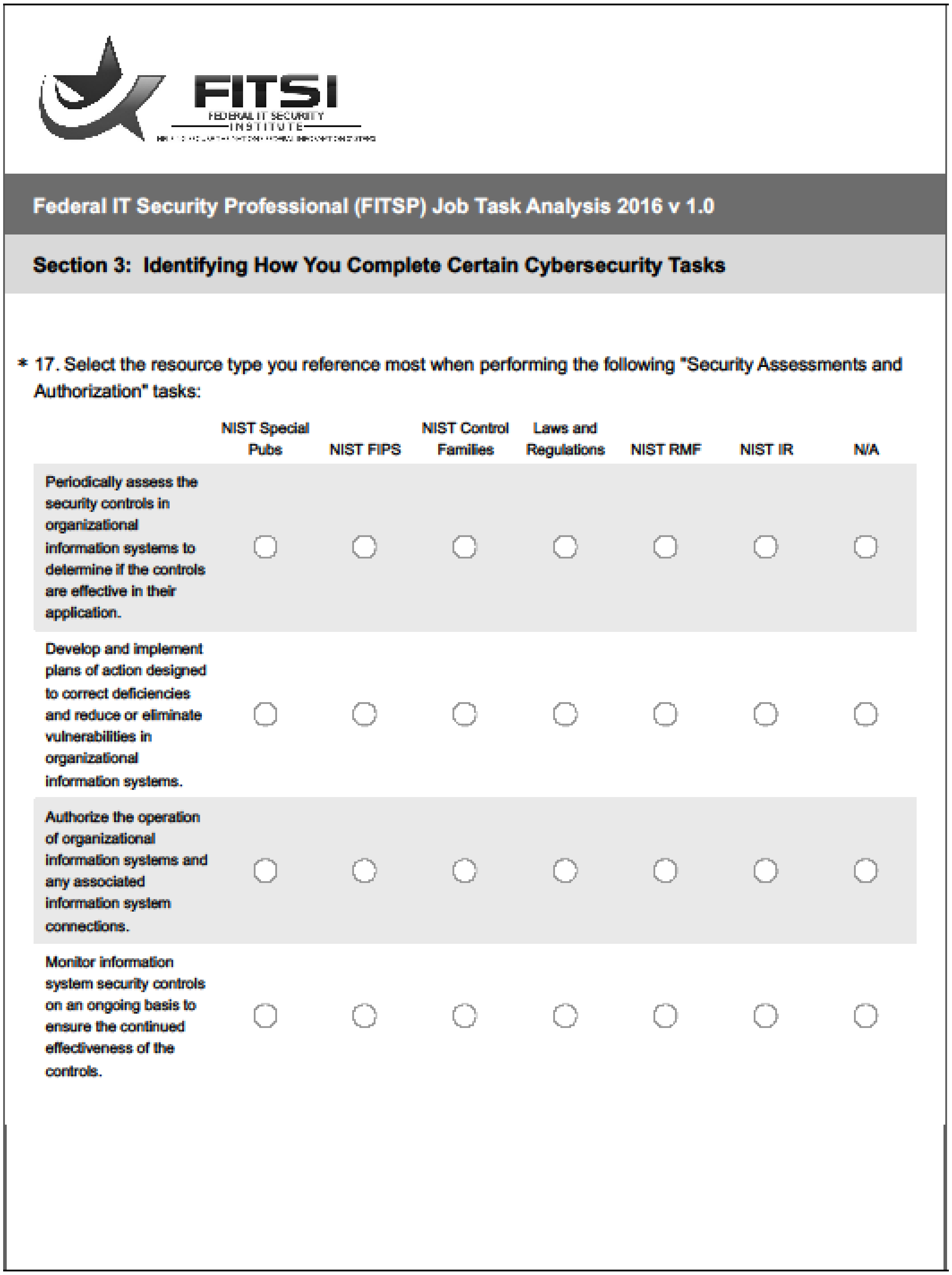


Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 16. Select the resource type you reference most when performing the following "Risk Assessment" task:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.	○	○	○	○	○	○	○



FITSI

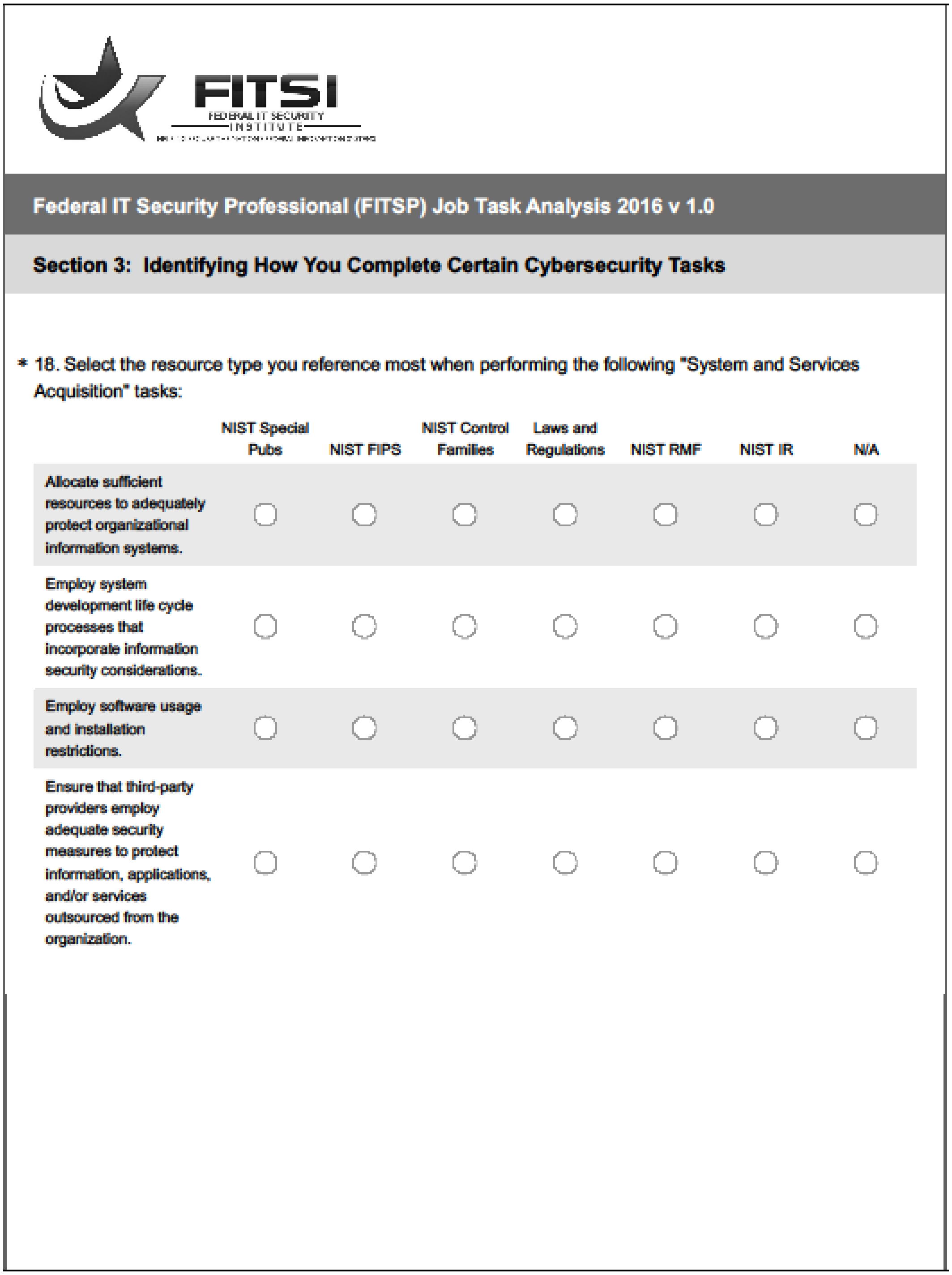
FEDERAL IT SECURITY INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 17. Select the resource type you reference most when performing the following "Security Assessments and Authorization" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	○	○	○	○	○	○	○
Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	○	○	○	○	○	○	○
Authorize the operation of organizational information systems and any associated information system connections.	○	○	○	○	○	○	○
Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	○	○	○	○	○	○	○

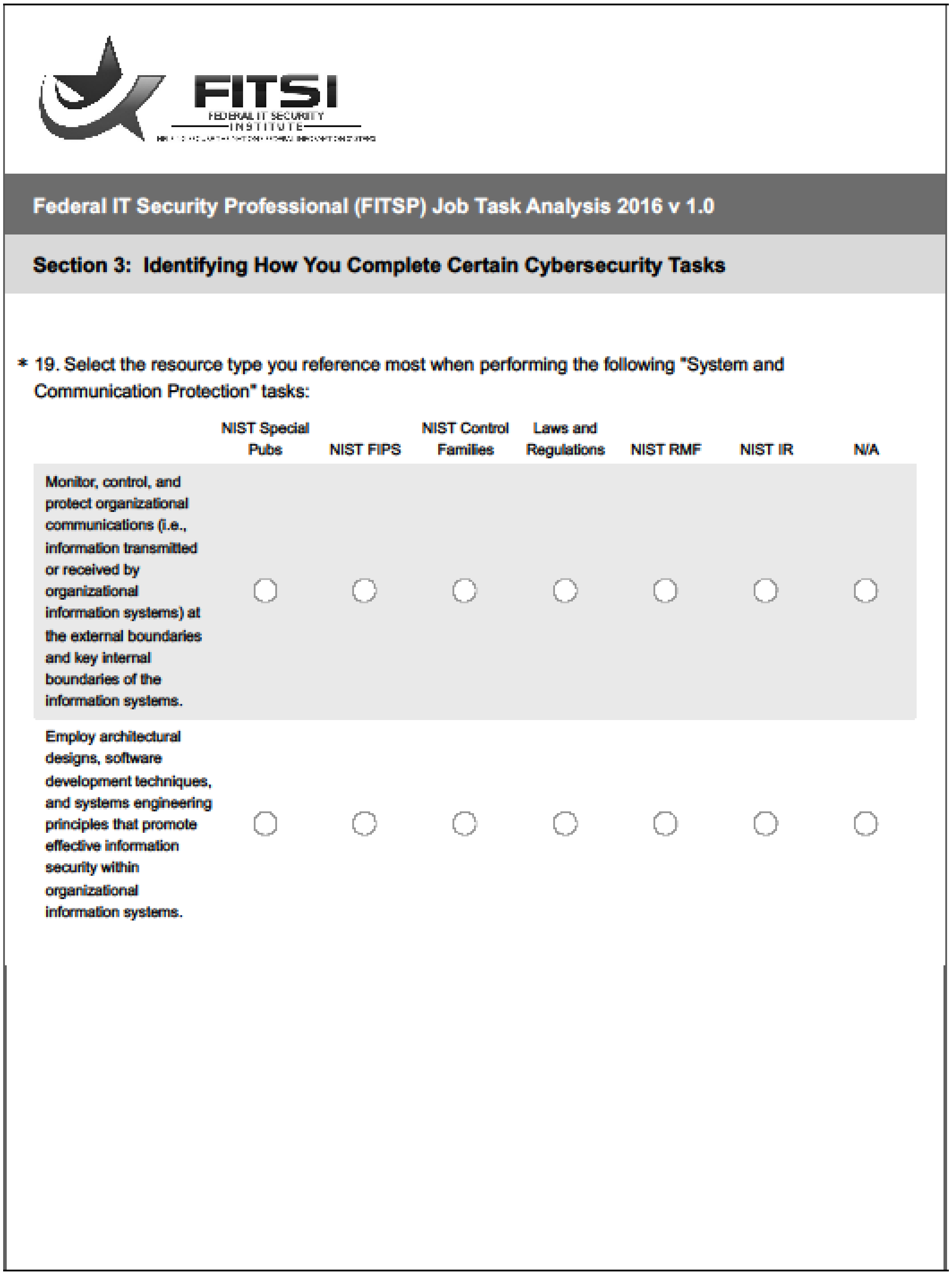


Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 18. Select the resource type you reference most when performing the following "System and Services Acquisition" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Allocate sufficient resources to adequately protect organizational information systems.	○	○	○	○	○	○	○
Employ system development life cycle processes that incorporate information security considerations.	○	○	○	○	○	○	○
Employ software usage and installation restrictions.	○	○	○	○	○	○	○
Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.	○	○	○	○	○	○	○



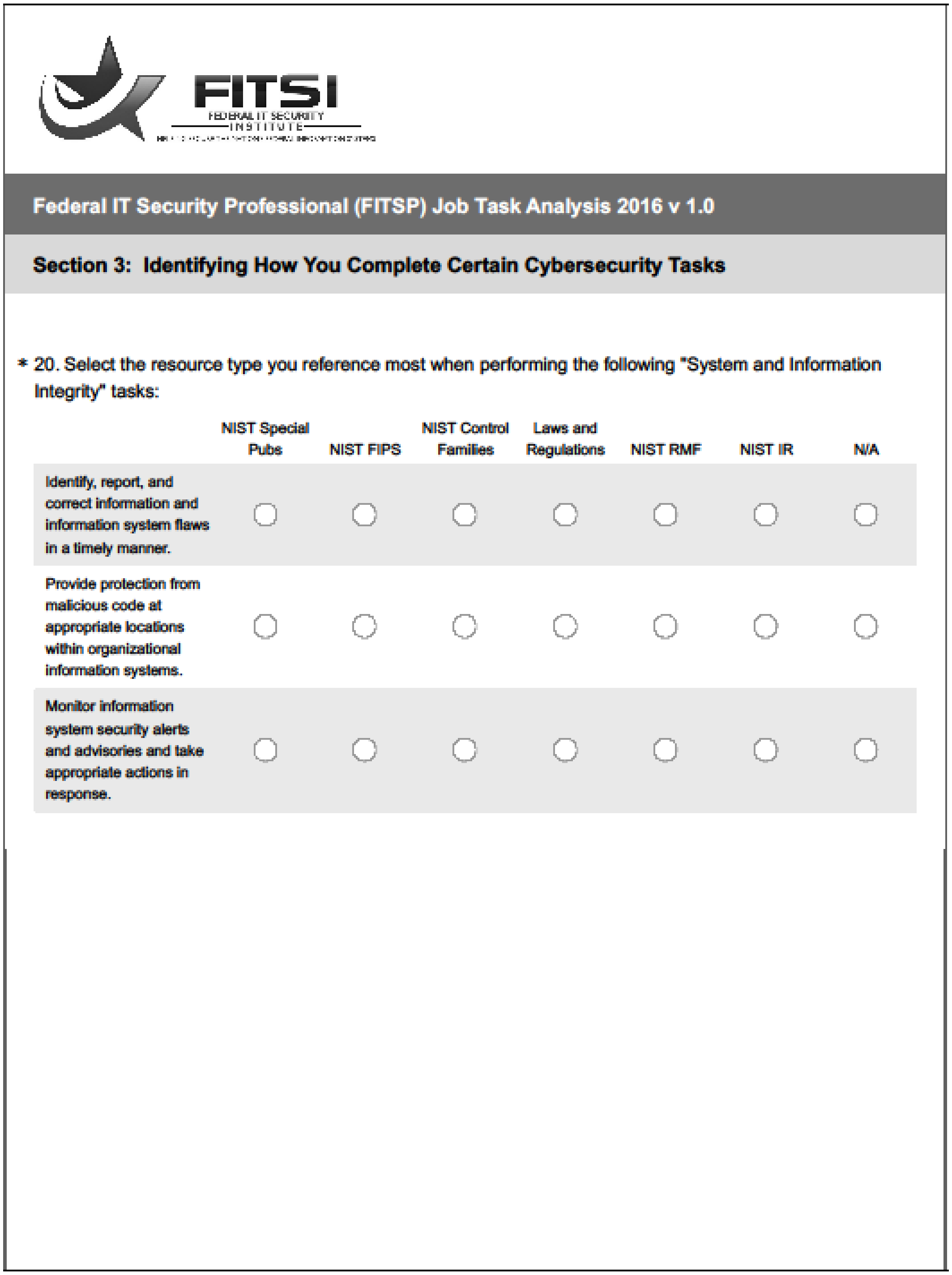
FITSI
FEDERAL IT SECURITY
INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 19. Select the resource type you reference most when performing the following "System and Communication Protection" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	○	○	○	○	○	○	○
Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	○	○	○	○	○	○	○



FITSI

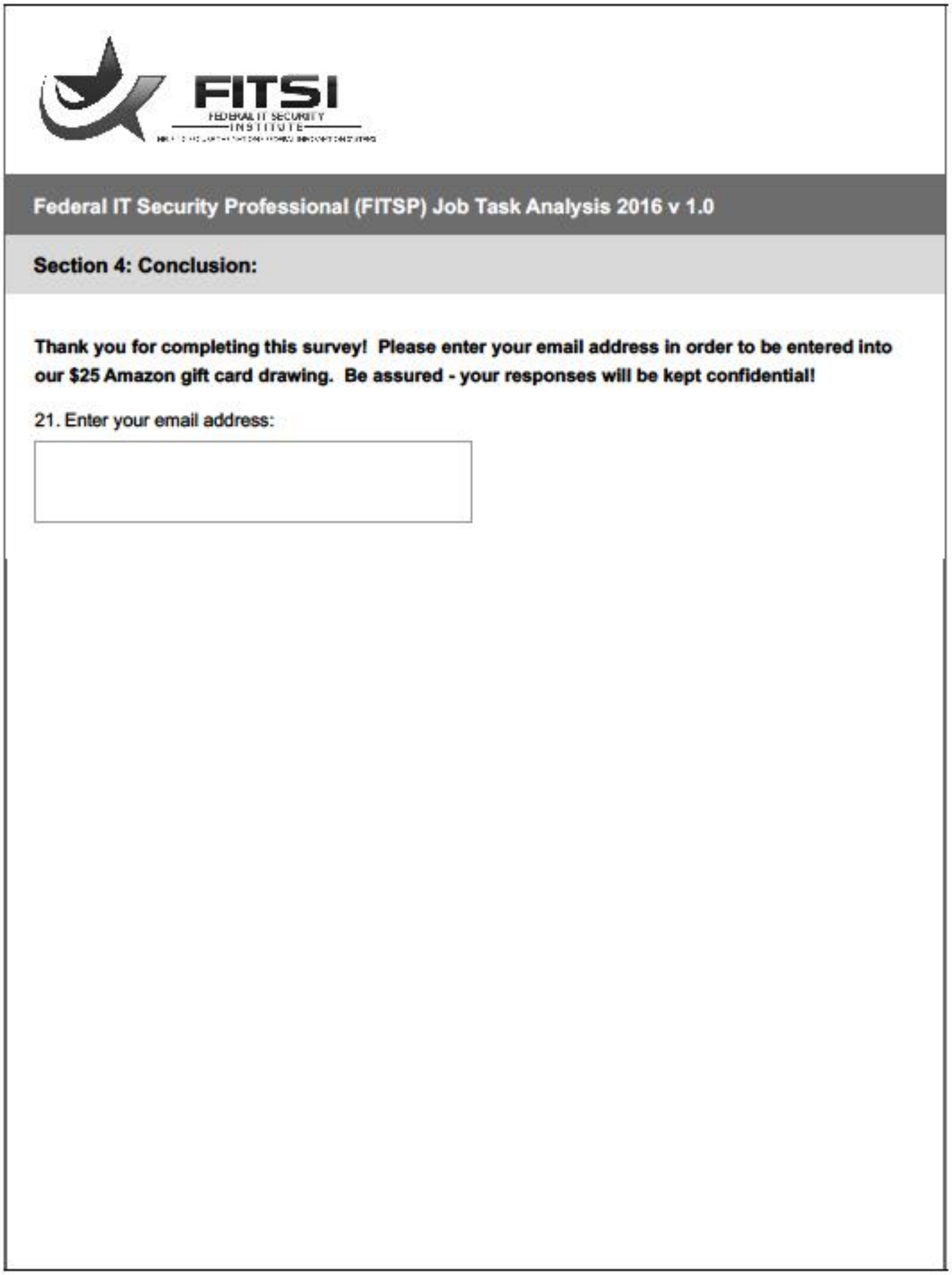
FEDERAL IT SECURITY INSTITUTE

Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 3: Identifying How You Complete Certain Cybersecurity Tasks

* 20. Select the resource type you reference most when performing the following "System and Information Integrity" tasks:

	NIST Special Pubs	NIST FIPS	NIST Control Families	Laws and Regulations	NIST RMF	NIST IR	N/A
Identify, report, and correct information and information system flaws in a timely manner.	○	○	○	○	○	○	○
Provide protection from malicious code at appropriate locations within organizational information systems.	○	○	○	○	○	○	○
Monitor information system security alerts and advisories and take appropriate actions in response.	○	○	○	○	○	○	○



Federal IT Security Professional (FITSP) Job Task Analysis 2016 v 1.0

Section 4: Conclusion:

Thank you for completing this survey! Please enter your email address in order to be entered into our $25 Amazon gift card drawing. Be assured - your responses will be kept confidential!

21. Enter your email address: