


FITSI Certification Holder Handbook



Requirements for
Maintaining
The Federal IT
Security Institute
(FITSI) Sponsored
Certifications

Version 2.1

Published 4/14/2020



This page is left intentionally blank

TABLE OF CONTENTS

1. OVERVIEW	4
2. APPLICABILITY	5
3. ONGOING CERTIFICATION REQUIREMENTS	6
4. USING THE PRIVATE PORTAL	7
5. CONTINUING PROFESSIONAL EDUCATION	9
A. WHAT IS A CPE?	9
B. CPE REQUIREMENTS	9
C. WHERE TO LOG CPE UNITS	9
D. QUALIFYING ACTIVITIES	11
E. CPE DOCUMENTATION	12
F. NON-COMPLIANCE	13
G. CERTIFICATION SUSPENSION AND CERTIFICATION WITHDRAWAL (REVOCATION)	13
H. CERTIFICATION REINSTATEMENT	14
6. USE OF THE FITSI CERTIFICATION LOGO	15
7. REQUEST FOR CERTIFICATION DUPLICATES	16
8. FITSI CODE OF ETHICS	17
A. THE COMPLAINT PROCESS	17
9. RECERTIFICATION REQUIREMENTS	19
10. RESIGNATION OF CERTIFICATION	20
11. APPEALS	21
12. FORMS	22
APPENDIX A, FITSI CONTACT INFORMATION	23
Figure 1: The FITSI Private Portal Login Screen	7
Figure 2: Reporting CPE Units Using the FITSI Portal	10
Figure 3: CPE Management Page	11

1. Overview

Congratulations on earning your Federal IT Security Professional (FITSP) Certification! We welcome you to the FITSP Certification Program. The Federal IT Security Institute (FITSI) was founded in 2009 to help secure the Nation's federal information systems by certifying that the federal workforce (civilian personnel, military, and contractors) understands and can apply appropriate federal Information Technology (IT) security standards. FITSI has many certification holders and members around the world, and we are pleased you are a part of this exciting group. While it is not a requirement to become a FITSI member to hold a FITSP certification, we recommend you consider the benefits of membership. More information can be found at <http://www.fitsi.org>.

FITSI is an Internal Revenue Service (IRS) Code section 501(c)(6) non-profit membership organization that is supported by exam and annual maintenance fees (AMF) from its certification holders and members. FITSI was established to help provide a certification scheme for the federal IT security workforce in the United States. Candidates can pursue up to four certification roles that are commonly found in federal agencies in the United States government (Manager, Designer, Operator, and Auditor).

2. Applicability

This handbook applies to all FITSP Certification Holders and provides pertinent information regarding the management and maintenance of your FITSP certification.

The most up-to-date *FITSI Certification Holder Handbook* can be found at <http://www.fitsi.org/documents.html>.

3. Ongoing Certification Requirements

Your FITSP certification is valid for three years from the date of issue. The issue date can be found on the certification and FITSI identification (ID) card. To maintain the currency of a FITSP certification, the certification holder must:

- Earn a minimum of 20 Continuing Professional Education (CPE) units each year. A FITSP Certification Holder reports annual CPE units using their individual private portal login information at <http://www.fitsi.org>. A total of 60 CPE units must be reported for the three-year certification cycle. These CPE units must be earned and reported within 30 calendar days of the anniversary date of certification. See Section 4 below for more information.
- Pay an AMF. The *FITSI Fee Schedule* can be found at <http://www.fitsi.org/documents.html>.

The FITSI Audit Committee conducts audits of reported CPE units as part of an oversight and validation program to ensure that reported CPE units are relevant to the industry and are appropriately quantified. All certification holders must maintain sufficient supporting documentation, as discussed in Section 4 of this handbook, to validate reported CPE units. Though all certification holders must retain this documentation, not all certification holders will be audited during any given certification cycle. Appropriate supporting documentation enables the Audit Committee to quickly and efficiently complete their review.

Certification holders are notified by email and asked to email appropriate documentation for review when selected for an audit. Upon successful completion of the audit, the FITSP Certification Holder is notified of the findings. If additional documentation is necessary, the auditor will notify the certification holder.

4. Using the Private Portal

As a FITSP Certification Holder, you will have access to the FITSI private portal. You will receive your unique login information to the portal around the time you receive your Certification Packet welcome packet. The login information will be sent to the email address that was entered during exam registration. If you fail to receive this email, please contact FITSI at contactus@fitsi.org with the words PORTAL LOGIN in the subject area. You will need to provide the following information:

- Full Name
- Mailing address used for registration
- FITSI ID and Certification numbers (found on your FITSI ID card)
- Preferred email address for FITSI use

Once you receive your private portal login information, you can access the FITSI private portal via the *Account Login* section of <http://www.fitsi.org>. The login screen will look like this:

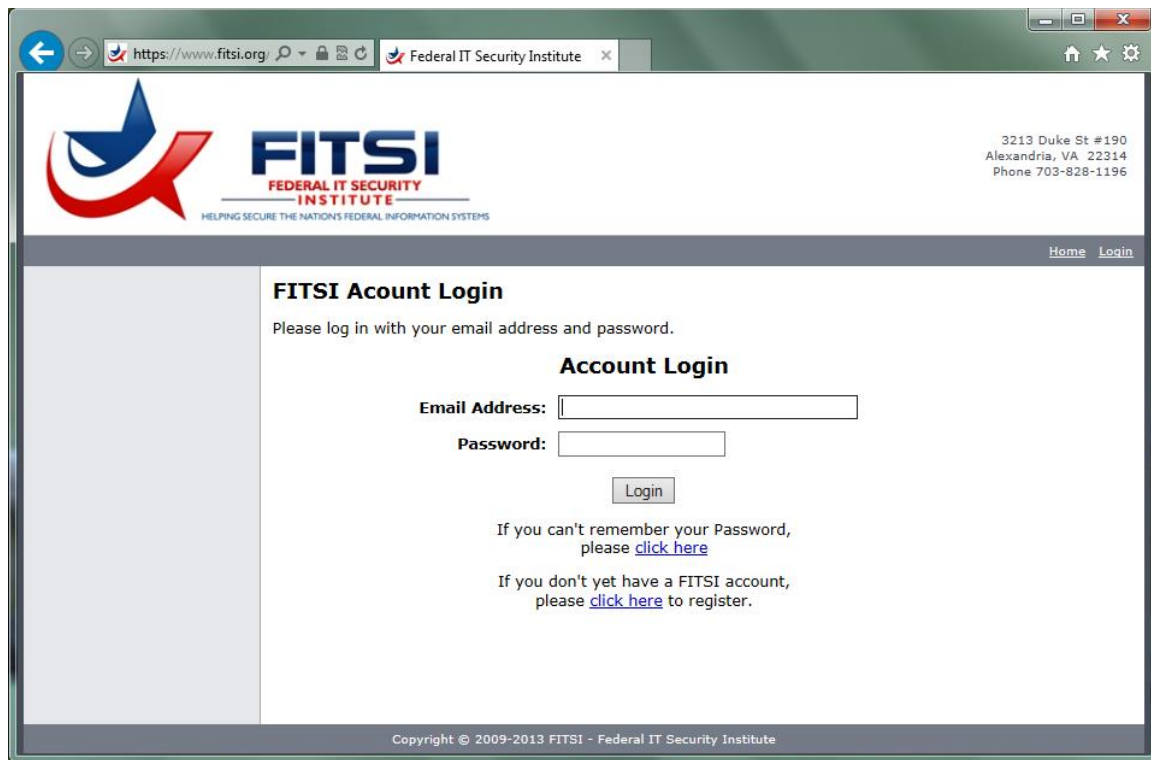
A screenshot of a web browser displaying the FITSI Private Portal Login Screen. The browser's address bar shows the URL <https://www.fitsi.org>. The page features the FITSI logo on the left, which includes a stylized red and blue graphic and the text "FITSI FEDERAL IT SECURITY INSTITUTE HELPING SECURE THE NATION'S FEDERAL INFORMATION SYSTEMS". On the right, contact information is provided: "3213 Duke St #190 Alexandria, VA 22314 Phone 703-828-1196". Below the logo and contact info, there are links for "Home" and "Login". The main content area is titled "FITSI Account Login" and contains the instruction "Please log in with your email address and password." Below this, there is a section titled "Account Login" with two input fields: "Email Address:" and "Password:". A "Login" button is positioned below the password field. Two lines of text provide additional instructions: "If you can't remember your Password, please [click here](#)" and "If you don't yet have a FITSI account, please [click here](#) to register." The footer of the page reads "Copyright © 2009-2013 FITSI - Federal IT Security Institute".

Figure 1: The FITSI Private Portal Login Screen

The *Member and Certification Holder Services* section allow the certification holders to complete a host of services items. Such items include, but are not limited to:

- Update profile information
- Record CPE units
- Join the FITSI evangelist program

FITSI provides certification holders and members the option to include contact information in an online directory via the FITSI private portal. The type and scope of information published is controlled by the certification holder or member through their online account profile. When a new online account is created, the default policy is set to "Not Published." The user can indicate the type of information they wish published in the directory.

FITSI may, from time to time, employ a third-party vendor to provide information to the FITSI certification holder base. In this event, FITSI will only authorize the vendor a one-time use privilege regarding certification holder data. FITSI does not sell, rent, or distribute personal information at any time.

No person may solicit or use the official FITSI certification holder list for any commercial purpose. This action is in direct violation of the FITSI Privacy Policy. Failure to follow this policy will result in a revocation of certification. The FITSI Privacy Policy can be found at <http://www.fitsi.org/privacypolicy.html>.

Individuals who feel personal information has been misused should contact the FITSI Corporate Office immediately. Contact information for FITSI can be found in Appendix A.

5. Continuing Professional Education

As stated above, each FITSP Certification Holder must earn and report 60 CPE units per certification lifecycle (three years). This section provides details about FITSP certification CPE requirements.

A. What is a CPE?

CPE units are obtained through the completion of activities that demonstrate the growth and development of skills related to one's profession. Typically, one CPE unit is equivalent to one hour of activity in pursuit of additional industry knowledge and experience.

It is important to understand that CPE units are earned outside of one's day-to-day employment activities. Activities that are directly related to a job do not qualify as CPE units. If a FITSP Certification Holder conducts the activity within the scope of normal job responsibilities, that activity cannot be used for CPE credit.

While the activities that qualify for CPE credit must be outside the scope of an individual's day-to-day work-related responsibilities, this does not mean the activity must occur outside of regular work hours to qualify as a CPE unit. For example, a FITSP Certification Holder may attend a security-related conference that is conducted during the certification holder's regular work hours. In this situation, the certification holder may use this as an opportunity to earn CPE credit. While the activity occurs during regular working hours, because it is outside the scope of typical work-related responsibilities and contributes to the professional development of the FITSP Certification Holder, this activity can be used to earn CPE credit.

B. CPE Requirements

Each certification holder must earn a minimum of 60 CPE units during each three-year cycle for each FITSP certification held. A minimum of 20 CPE units must be earned each year. These CPE units must be reported within 30 calendar days of the anniversary of the original date of certification.

For example, if John Doe earned the FITSP-Manager credential on January 1, 2011, his certification is valid until January 1, 2014. He has until January 30, 2012, to earn and report 20 CPE units for year one, January 30, 2013, for year two, and January 30, 2014, for year three.

C. Where to Log CPE Units

CPE units are reported at the private portal using the *Manage CPEs* interface in the *Member and Certification Holders Services* section. See Section 3 for more information on the private portal. Figure 2 illustrates the reporting process.

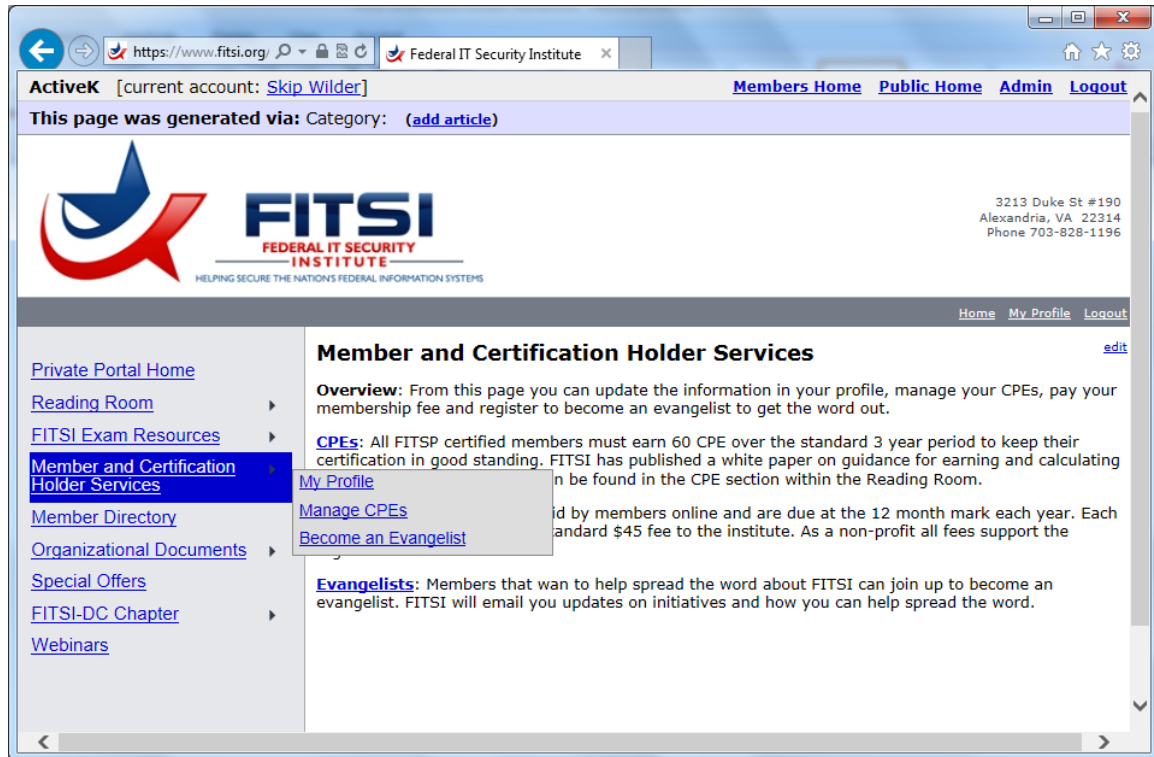


Figure 2: Reporting CPE Units Using the FITSI Portal

Using the *Manage CPEs* interface, certification holders perform CPE management actions. Figure 3 shows an overview of this interface. Reminder: FITSP Certification Holders should plan on reporting 20 CPE units per year through this interface to keep each FITSP certification held current.

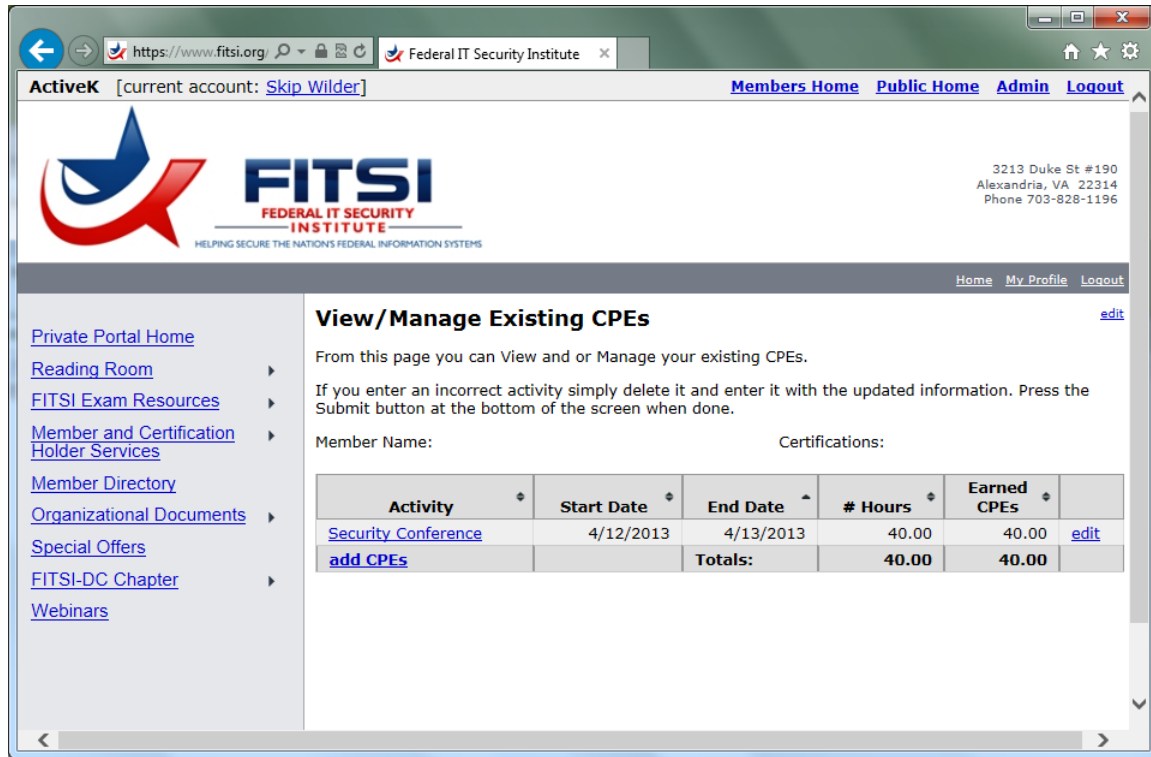


Figure 3: CPE Management Page

D. Qualifying Activities

Certification holders may pursue a wide range of activities to earn CPE credit. All professional activities must be completed outside of typical job-related responsibilities and must contribute to professional development in IT security. One CPE unit can be earned for each hour of related activity.

Activities that certification holders can use to qualify for CPE units are listed below.

- Attend security conferences – One CPE unit for each hour of IT security discussion covered in the conference
- Attend security training classes – One CPE unit for each hour of instruction. These classes can be instructor lead, online, or computer-based training modules.
- Publish security whitepapers – One CPE unit for each hour spent writing a whitepaper, not to exceed five CPE units per the published whitepaper
- Publish security books – One CPE unit for each hour spent writing a book, not to exceed 30 CPE units per published book
- Teach IT security training classes – Three CPE units for each hour of in-class time
- Read IT security books – One CPE unit for each hour of reading a book, not to exceed five CPE units per book
- Provide National Institute of Standards and Technology (NIST) commentary on draft documents – One CPE unit for each hour spent working on submitting commentary, not to exceed five CPE units per activity

Examples:

1. Example #1 – Attending a security conference: conference time is broken down into the number of hours of the conference. For a 35-hour conference (five days), the FITSP Certification Holder can report 35 CPE units for this activity.
2. Example #2 – Taking a college-level course (college-level courses are based on in-class time): a class meets one day a week for ten weeks and includes 1.5 hours of instruction, which would result in 15 CPE units (10 X 1.5 = 15).
3. Example #3 – Reading an IT security book: a certification holder reading an IT security book can report one CPE unit for each hour of reading, up to five CPE units.

E. CPE Documentation

FITSP Certification Holders must retain documentation of completion of the activity being reported for CPE credit. This documentation may be requested by the Audit Committee if the certification holder is selected for audit. Documents that should be retained for each type of activity are:

1. Attend security conferences
 - a. Receipt showing payment of conference and name of attendee
 - b. Conference guide provided to attendee detailing speakers and topics discussed – should also include the time the certification holder spent in conference sessions
 - c. Conference completion certificate (if provided)
2. Attend security training classes
 - a. Receipt showing payment for course and name of attendee (free classes need a confirmation email or communication in place of a receipt)
 - b. Course name and description
 - c. Course syllabus
 - d. A document detailing the number of hours the certification holder spent in class
 - e. Course completion certificate
3. Publish security whitepapers
 - a. Whitepaper name
 - b. Detailed log of time spent preparing the whitepaper
 - c. A copy of the published whitepaper and reference for where it can be located (such as a website URL)
4. Publish security books
 - a. Book name, author, publication date, and International Standard Book Number (ISBN) number
 - b. Detailed log of time spent writing and editing the book
5. Teach IT security training classes
 - a. Course name and description
 - b. Course syllabus
 - c. Course timeline indicating time spent in class conducting class (CPE units are calculated as three times the total hours spent teaching the class)
6. Read IT security books
 - a. Book name, author, publication date, and ISBN

-
- b. Detailed log of time spent reading the book
 - c. A summary of lessons learned from the book related to the reader's FITSP certification area
 7. Provide NIST commentary about draft IT security documents
 - a. List titles of the draft document reviewed
 - b. Copy of commentary provided to NIST
 - c. Detailed log of time to complete analysis and draft commentary

The certification holder should retain this documentation for full accountability in the event of a CPE audit. Upon completion of the three-year cycle, and recertification of qualifications by FITSI, retention of the documentation for the previous three-year cycle is not required.

F. Non-Compliance

A certification holder will be declared to be in a non-compliant state for failure to report the requisite CPE units each year or failure to pay the necessary AMF. For this reason, it is essential that all FITSP Certification Holders report at least 20 CPE units each year for each FITSP certification held.

G. Certification Suspension and Certification Withdrawal (Revocation)

FITSI certification holders must keep their certifications in good standing for the current three-year cycle. A FITSI certification can be suspended or withdrawn (revoked) for a certification holder due to non-compliance with the certification maintenance requirements.

A certification may be put into a suspended state for the following reasons:

- Failure to stay current with Annual Maintenance Fees (AMFs)
- Failure to report of necessary CPEs.
- Having a complaint against a certification holder for violation of the FITSI Code of Ethics.

The suspension period can last for up to 90 days. During this time, the certification holder must refrain from further promotion of the certification while it is suspended. To remove the certification from a suspended state, the certification holder will need to address the issue causing the suspension to occur.

If the certification holder does not address the issue causing the suspension to occur after 90 days, the certification will be withdrawn (revoked).

Reasons for withdrawal (revocation) of the certification are:

- Continued failure to bring outstanding AMFs current after 90 days
- Continued failure to report necessary CPEs after 90 days
- Having been found through the complaint process to violate the FITSI Code of Ethics.

In a case a certification is withdrawn (revoked), the certification holder must discontinue the use of all claims and references to the certification, and discontinue use of the FITSI Certification Logo.

H. Certification Reinstatement

A withdrawn (revoked) certification can be reinstated up to 18 months from the date of withdrawal by submitting a *FITSI Certification Reinstatement Application*. Additional fees and penalties apply. This form can be found at <http://www.fitsi.org/documents.html>.

A certification holder who has had their certification withdrawn for violation of the FITSI Code of Ethics cannot have their FITSI certification reinstated.

6. Use of the FITSI Certification Logo

An individual who has been granted a FITSP certification may list the specific certification on stationary, websites, resumes, business cards, and other promotional materials. Any individual who has a certification revoked must discontinue the use of the FITSI Certification Logo while the certification is in a (withdrawn) revoked status.

Certification should appear as:

First name, Last name, Federal IT Security Professional – *Role*

or

First name, Last name, FITSP – *Role*

Where *Role* indicates the area of expertise certified in: Designer, Operator, Manager, or Auditor.

For example, if Mary Jones earned her FITSP certification as an Operator, she would indicate it by:

Mary Jones, Federal IT Security Professional – Operator

or

Mary Jones, FITSP – Operator

7. Request for Certification Duplicates

A certification holder may request additional copies of a certificate or FITSI ID card. The *FITSI Fee Schedule* provides the most current duplicate copy fees and can be found at <http://www.fitsi.org/documents.html>. The request for a duplicate should be emailed to contactus@fitsi.org.

Requests for duplicates will be fulfilled within 30 calendar days of receipt.

8. FITSI Code of Ethics

All FITSP Certification Holders must abide by the FITSI Code of Ethics, which can be found in the *FITSI Code of Ethics Handbook* at <http://www.fitsi.org/documents.html>. Violations of any tenet of the FITSI Code of Ethics may be grounds for revocation of a certification holder's FITSP certification(s) and possibly FITSI membership (where applicable).

FITSI can only be as good as its representative base. If a FITSP Certification Holder is believed to violate the FITSI Code of Ethics, a complaint may be submitted to the FITSI Corporate Office. Individuals may file a complaint against a certification holder at any time.

A. The Complaint Process

Complaints can be lodged against FITSI for the following areas:

- Complaint regarding examination items
- Complaint regarding the examination process
- Complaint regarding specific exam circumstances
- Complaint against any FITSI Board Member, Associate Member, Certified Member, Founding Member, or certification candidate the complainant feels is in violation of any FITSI policy
- Other issues

A complaint can be filed by submitting the *Complaint Form* in the *FITSI Appeals and Complaint Application*, which can be found at <http://www.fitsi.org/documents.html>. The completed form should be emailed to FITSI at contactus@fitsi.org.

All complaints must be submitted with supporting information. The FITSI Appeals Committee will review the nature of the complaint and render a decision on the complaint within 60 calendar days of receipt. Each complainant will receive the Appeals Committee's decision or recommendation.

The response from the Appeals Committee will be one of the following:

- Complaint denied
- Complaint accepted
- Request for more information

Responses may include a detailed explanation of the response. All decisions made by the Appeals Committee are considered final.

In the event a complaint against a certified person is substantiated by the Appeals Committee, the Certification Director will send a memo notifying the subject of the complaint about the complaint within 30 days of the Appeals Committee decision.

Any information provided to FITSI will be treated confidentially, and the identity of the complainant will not be revealed to the accused without prior permission of the complainant.

9. Recertification Requirements

The FITSP certification is valid for three years. FITSP Certification Holders may renew a certification that is at the end of the three-year cycle for an additional three-year cycle.

Certification holders must meet the following requirements to be eligible for renewal:

- Candidates must have earned and reported a total of at least 60 CPE units (per certification role) over that certification's three-year life cycle.
- Candidates must have passed the FITSI internal CPE audit (if chosen).
- Candidates must not violate any part of the FITSI Code of Ethics or have an active complaint filed in his or her name.
- Candidates must be current with their AMF.

10. Resignation of Certification

A FITSP Certification Holder may resign by filing a written resignation with the FITSI Corporate Office. Resignation does not relieve an individual of unpaid dues or other charges previously incurred. Any person resigning a certification may be required to return the FITSI ID card, challenge coin, and certification certificate.

11. Appeals

Any decision rendered by a FITSI committee, staff member, or consultant that impacts a FITSI member, candidate, or FITSP Certification Holder may be appealed through the FITSI Appeals Committee. All appeals must be made within 30 calendar days of the receipt of the decision being appealed.

Appealable decisions include:

- Certification Denial
- Certification Revocation
- Refund Refusal
- Other decisions or issues

An appeal must be filed by submitting the *Appeals Form* in the *FITSI Appeals and Complaint Application*, which can be found at <http://www.fitsi.org/documents.html>. The completed form should be emailed to FITSI at contactus@fitsi.org.

Once an *Appeals Form* is received, FITSI will carry out the following steps:

1. **Initial Appeal Acknowledgement.** The Appeals Committee will acknowledge receipt of the appeal within 30 calendar days of receipt. The email acknowledgment will include:
 - Explanation of the appeals process for the issue at hand
 - The Appeals Committee member point of contact
 - A timeline for response and decision by the Appeals Committee
2. **Appeals Review.** The Appeals Committee will render a decision within 30 calendar days of receipt of the appeal unless additional information is required. In the event additional information is required, the Appeals Committee will render a decision within 30 calendar days of receipt of the required information. The decision will be provided via email to the appellant.
3. **Appeals Decision/Response.** The Appeals Committee response will be either appeal accepted or appeal denied. All responses will include a detailed explanation of the decision.
4. **Appeals Escalation.** All decisions made by the Appeals Committee are considered final.

The submission of the appeal and subsequent investigation and decision shall not result in any discriminatory actions against the appellant.

12. Forms

The most current version of the forms referenced in this handbook can be downloaded from <http://www.fitsi.org/documents.html>.

Appendix A, FITSI Contact Information

FITSI Corporate web site address:

<http://www.fitsi.org>

FITSI Corporate Office:

Federal IT Security Institute (FITSI)

3213 Duke St.

Suite 190

Alexandria, VA 22314

Phone: 703-828-1196

Fax: 703-754-8215

Web site: <http://www.fitsi.org>

General Email: contactus@fitsi.org