

# Military Education & Career Development

IN THE FEDERAL GOVERNMENT



CALIFORNIA INSTITUTE OF  
ARTS & TECHNOLOGY

## **ACKNOWLEDGMENTS**

*This thought leadership paper is a joint project between the **California Institute of Arts & Technology** and the **Foundation for Women Warriors**.*

*Written by John Gormally*

*Designed by Karina Svityashchuk*

# Table of Contents

---

Introduction .....4

Key Terms to Know for Cybersecurity Careers in  
the Federal Government.....6

What are the Entry-Level Cybersecurity Roles  
Supporting the Federal Government?.....12

What are the Various Federal Security  
Clearances?.....17

What is the Role of a Certified Ethical Hacker in  
the Federal Government?.....22

Managing Secured Data for the Federal  
Government.....25

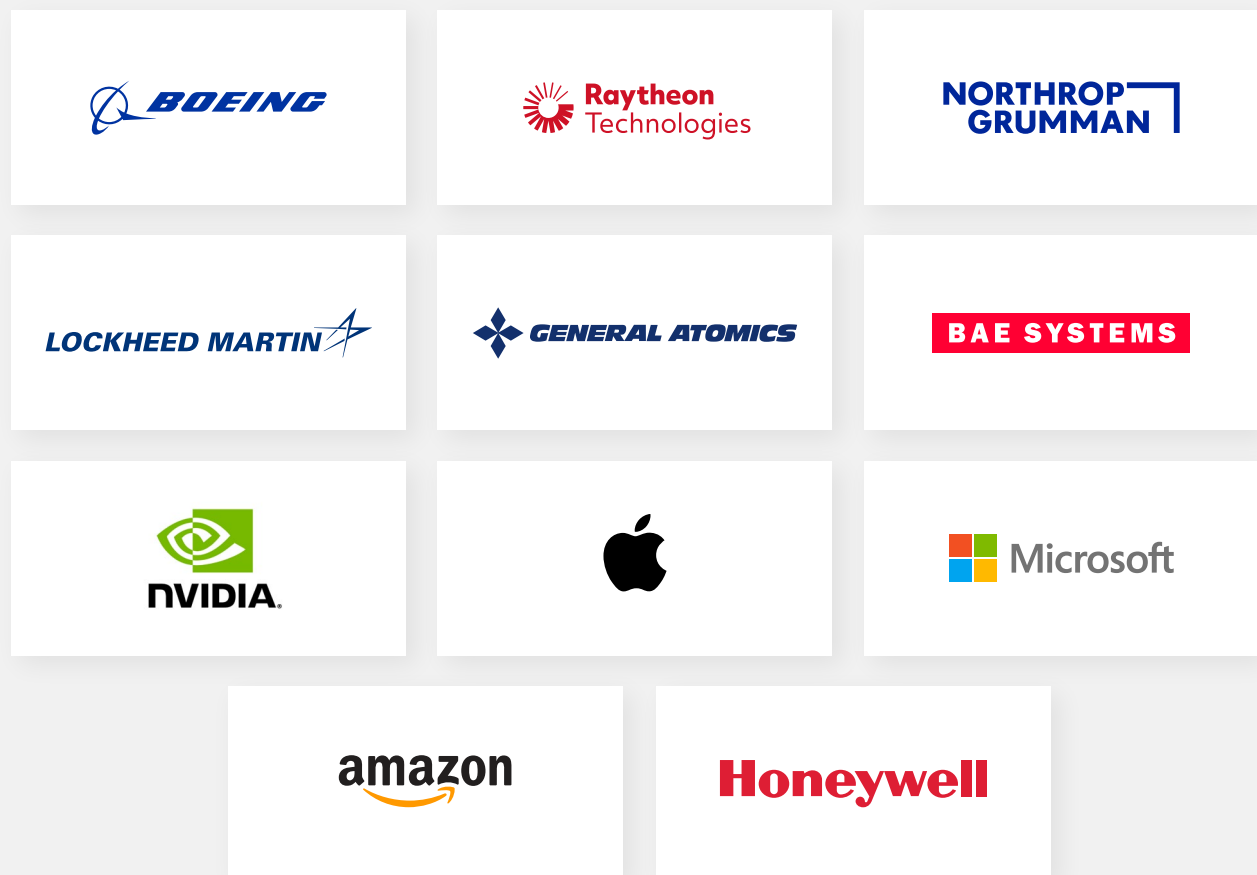
What is FedRAMP?.....30

What are the Implications of  
CMMC in 2023?.....34

Take the First Step.....37

Opportunities for people to develop or enhance their skills and experience with Science, Technology, Engineering, and Math (STEM) remain available in every state. For those either serving or planning to depart military service, many resources are available to help with your transition into data analytics, cybersecurity, and computer science careers.

Veterans today should consider applying for these exciting roles in STEM within the various U.S. Federal Government agencies and departments or possibly with one of the Military Industry Base (MIB) members, including:



These organizations often recruit former military personnel to help fill the thousands of open positions throughout the defense contractor space. Both military men and women should invest time in researching these companies and how their experience, training, and leadership skills could be an asset to them. These members of the MIB have recruiters focused on meeting with current and former active duty personnel to help with their transition into civilian life.

This paper will provide insight into the hiring processes of the Federal Government, including:

- ✓ What are the various security clearances required?
- ✓ What are the various cybersecurity frameworks all candidates should be aware of?
- ✓ What courses/degrees/certification programs should I consider?
- ✓ What roles in the Federal Government should I apply for?
- ✓ What is the payscale for Federal employees?
- ✓ Will my Military time-in-service be considered if I accept a role in the Government?
- ✓ Is their career counseling and financial aid available for women veterans?








# Key Terms to Know for Cybersecurity Careers in the Federal Government

---

Working in the United States Federal Government, especially in Cybersecurity, can be very challenging for people unfamiliar with the frequently used acronyms and terms.

These acronyms and terms are used because many Federal Agencies have long program or mandate titles. For example, the acronym HIPAA stands for Health Insurance Portability and Accountability Act.

CIAT.edu also offers multiple programs that can prepare students for Cybersecurity or Data Analytics careers in the Federal Government:

-  **Applied Bachelor's Degree in Computer Information Systems–Cybersecurity Concentration**
-  **Applied Bachelor's Degree in Software Development–Data Analytics Concentration**
-  **Certified Ethical Hacker (CEH) Certification–CEH–V11**

This section helps highlight the most common Federal Cybersecurity terms, privacy mandates, and architectures all students should know before applying to any Federal Government position.

## What are the Key Cybersecurity Terms in the Federal Space?

Everyone studying Computer Science, Data Analytics, and Cybersecurity should become familiar with the critical terms widely used within the Federal Government. These terms and acronyms are often used in reports, budget meetings, and in dealing with external and internal cyber threats.

These terms include:

### **RISK**

*Risks are the potential harm or loss of data, personal, or government materials.*

### **ASSET AND INFORMATIONAL ASSETS**

*Assets or Informational Assets are high-priority physical or logical systems within the Federal Government.*

### **THREATS**

*Threats are considered events or expected actions by adversaries against U.S. Government personnel, resources, assets, and materials.*

### **THREAT SOURCES**

*Threat sources are the expected or unsuspected adversaries behind the threat.*

### **VULNERABILITY**

*Threat sources are the expected or unsuspected adversaries behind the A vulnerability is a possible exploitable, personal, or material system within the U.S. Government. Vulnerabilities follow CVE scoring to determine risk level before becoming exploited.*

○ **CONTROLS**

*Controls refer to physical, logical, or cyber-related control for protection, monitoring, and response to a threat, vulnerability, or intrusion.*

○ **LIKELIHOOD**

*Likelihood is a critical first step in the risk scenario workflow (Asset-Threat-Vulnerability), and the likelihood score is based on the expected impact of the event.*

Under the **Defense Federal Acquisition Regulation Supplement (DFARS)**, additional vital terms all students should know include:

○ **COMPROMISE**

*Defined as possible information theft or data exposure from unauthorized personnel.*

○ **CYBER INCIDENT**

*Defined as an actual threat executed with technology, not humans, resulting in the exploitation of a system or data exfiltration.*

○ **COVERED DEFENSE INFORMATION**

*Refers to a data classification based on sending data to third parties, including a defense contractor or approved foreign country.*

These binding terms are often referenced with the Federal Government's pillar strategy provided by the U.S. Department of Defense (DoD) and various security analysts who define risks. These pillars establish mandates and frameworks to protect the multiple data and network systems with a unified approach.



# What are the Four Pillars of Cybersecurity in the Federal Government?

The U.S. Department of Defense often provides specifics to the public about the Four Pillars and how they align with the overall Federal Government National Security Systems protection strategy.

These pillars include:

<b>Defend</b> Defend Critical Infrastructure specific to SaaS platforms and cloud services (FedRamp)	<b>Disrupt</b> Disrupt cyber terrorism activities through offensive and counter-offensive hacking operations (CHE)	<b>Compel</b> Compel the private industry and technology companies to develop more residence solutions to protect U.S. Government and private sector data (NIST)	<b>Invest</b> Invest in programs like the ones offered at <a href="https://www.ciat.edu">CIAT.edu</a> to help with the job shortage in the Computer Science, Data Analytics, and Cybersecurity fields.
---	---	---	---

## Which Department in the Federal Government Handles Cybersecurity Strategy?

The National Cybersecurity Strategy is a multi-layer complex strategy filled with terms defined by the Cybersecurity industry. Below is an outline of the various departments that handle this strategy.

### **DHS**

The Department of Homeland Security and its components promote cybersecurity resilience nationwide, investigate potential cyber threats, and safeguard cybersecurity along with democratic values and principles.

### **CISA**

The Cybersecurity and Infrastructure Security Agency (CISA) has developed a playbook, per the direction of Executive Order 14028, Section 6, to facilitate better plans and responses to cybersecurity incidents and vulnerabilities in Federal Civilian Executive Branch Information Systems.

## **NIST**

The National Institute of Standards and Technology (**NIST**) falls under the Department of Commerce. This agency creates several technology and cybersecurity standards for the Federal Government to unify. It mandated most Federal Government agencies to align with NIST standards.

Several government agencies developed security standards and policies. NIST unified the Federal Government with proven industry frameworks, architectures, and procedures to meet regulatory mandates. Non-government organizations also leveraged the NIST framework. Complying with NIST-800-53 also helped the organization streamline its governance requirements for PCI-DSS, HIPAA, and CCPA.

By understanding the laws and regulations governed by the Federal Government, students will see the critical importance of the various agencies' frameworks needed to ensure the networks and data stay protected.

# What are the Main Federal Cybersecurity Laws and Regulations?

## **THE COMPUTER FRAUD AND ABUSE ACT (CFAA)**

This is the primary statutory law for prosecuting cybercrime, such as hacking and extortionate crimes, like ransomware. It offers criminal and civil penalties, with the illegal range extending from 10 to 20 years imprisonment for aggravated offenses.

## **THE ELECTRONIC COMMUNICATIONS PROTECTION ACT (ECPA)**

The ECPA protects communications in transit and storage. The Stored Communications Act (Title II of the ECPA) states that accessing a facility offering an electronic communications service is a crime without authorization or exceeding such rights. Violations are punishable with up to 10 years in jail if done intentionally.

## **THE WIRETAP ACT (TITLE I OF THE ECPA)**

The Wiretap Act also forbids intercepting electronic communication and carries various exceptions for law enforcement, employer-based services, and service providers under some circumstances.

## THE ECONOMIC ESPIONAGE ACT OF 1996

The Economic Espionage Act of 1996, Defend Trade Secrets Act of 2016, and Wire Fraud statute impose penalties for unlawfully retrieving private intellectual property or proprietary information from trade secrets sources and economically motivated frauds committed through telephone wire systems.

# Knowledge for Today and in the Future

Many Federal departments have overlapping cybersecurity strategies. Some departments created cybersecurity standards and procedures to meet their needs.

With the adoption of NIST-800 as the standard for all Federal departments and agencies to align with, the unification of cybersecurity processes and strategy has become more realistic. Agencies like DHS, CISA, and NIST help define a strategy for the Federal Government and the private sector.

We encourage students looking to join the cybersecurity community supporting the Federal Government to familiarize themselves with terminology frequently used in the space and attend programs at [CIAT.edu](https://www.ciatt.edu) to learn the foundation of Computer Science, Cloud Security, and Data Analytics. These domains are used within the Federal Government and, of course, Cybersecurity.



# What are the Entry-Level Cybersecurity Roles Supporting the Federal Government?

---

The demand for qualified applicants for entry-level and advanced roles in cybersecurity to support the U.S. Federal Government continues to grow.

For Federal Government jobs, recent graduates with cybersecurity qualifications, holders of certifications related to Cybersecurity, and people possessing the right skills may not necessarily be required to have a master's degree to apply. However, many roles in the Federal Government may include comprehensive background investigations and a competitive selection process.

The Cybersecurity industry encourages students seeking a career in cybersecurity in the Federal Government to look into courses offered at CIAT.edu:

-  **Applied Bachelor's Degree in Computer Information Systems–Cybersecurity Concentration**
-  **CISSP Certification**
-  **CompTIA Security+ Certification**
-  **Certified Ethical Hacker (CEH) Certification–CEH–V11**
-  **AWS Security Specialty Certification**

These degree and certificate programs provided the needed foundation of knowledge to help students apply for entry-level roles within civil services jobs supporting the U.S. Government agencies, departments, and the Defense Industrial Base (DIB).

This section discusses entry-level positions, pay scale, cybersecurity job growth opportunities, and the Federal Government application process. Like the private sector, there continue to be more job openings than candidates for many opening positions in the Federal Government. Entry-level opportunities are there for students to pursue!

## The Federal Hiring Process

Although employing personnel in the Federal Government shares similarities with private enterprises, there are distinct differences due to applicable laws, executive orders, and regulations. Within the Federal application process, the candidate should review the various application deadlines, additional security checks, and any competitive examination requirements.

Most Federal positions are broken into several categories, including:

### **SERVICE**

*These positions, which involve competition, are subject to civil service laws that aim to ensure fair, open competition and selection based on an applicant's knowledge, skills, and abilities.*

### **EXCEPTED**

*Certain positions are designated as "Excepted Service" and subject to a distinct set of appointment, pay, and classification rules, which are different from those in the competitive service.*

### **MERIT**

*Employees who have been in a competitive appointment in the Federal Government for 90 days or more may be eligible to fill vacancies or job opportunities per the Veterans Employment Opportunities Act of 1998 when external candidates are accepted.*

Each of these hiring categories aligns with the Federal General Scale pay system.



# What is the GS Pay Scale System?

The General Scale (GS) system is a payment system for civilian employees in the Federal Government; evaluation and compensation vary by grade level. The qualification requirements for each position are based on education, background, accomplishments, and experience. In the job posting, your salary may become publicly available on sites such as FederalPay.org.

## Entry-Level & Advanced Federal PayScale

A General Schedule (GS) grade usually begins at Step 1; however, in some cases, an employee may be authorized to start at a higher step rate due to particular qualifications or agency requirements.

### **GS-3 OR GS-4**

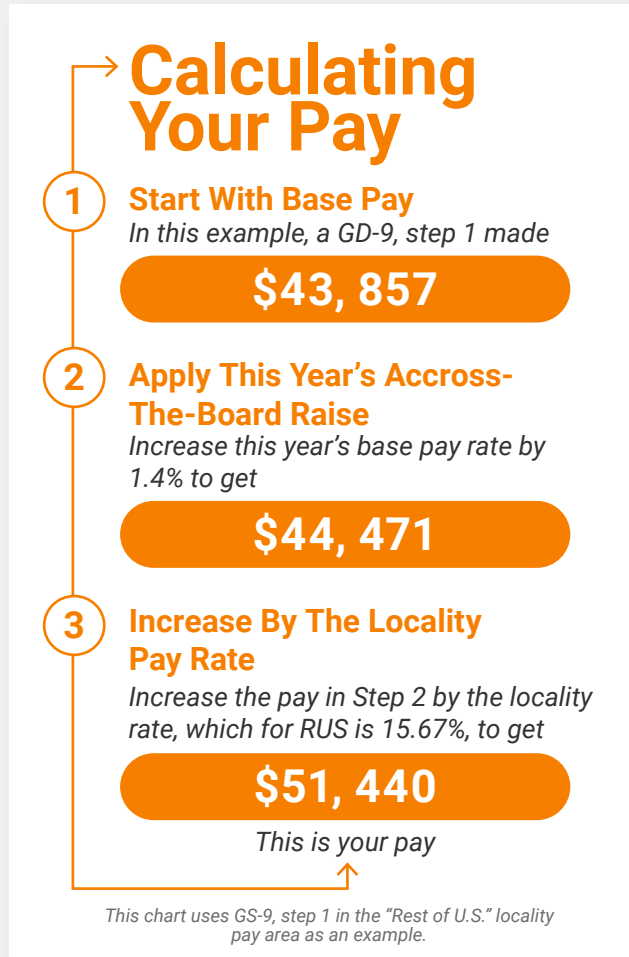
typically internships, student jobs, or lower-level administrative work

### **GS-5 TO GS-7**

mostly entry-level and administrative positions

### **GS-8 TO GS-12**

mostly mid-level technical and first-level supervisory positions



## Common Entry-Level & Advanced Cybersecurity Positions in the Federal Government

The Federal Government has several cybersecurity roles, including entry-level security operations to top-secret cryptography code breakers working for the National Security Agency. Each part has a pay scale, security clearance, and specific education requirements. Many of these positions cross between departments and agencies. This lateral movement gives students and entry-level

cybersecurity personnel options to move between government departments without losing time in grades toward retirement.

Many veterans leaving active-duty service are encouraged to apply for a Federal Government position. If accepted, their time-in-grade in military service carries forward into their new role.

Here is a sampling of entry-level and intermediate cybersecurity roles in the Federal Government:

### **CYBER INCIDENT RESPONSE ENGINEER**

This is an excellent entry-level role. A Cyber Incident Response Engineer works within the Security Operations teams. This group handles all incident responses and root cause analysis of a cyber attack, provides emergency patches and updates to systems, and monitors all security controls.

### **INFORMATION SECURITY ANALYST**

As an Information Security Analyst, you must be able to recognize and report security breaches in a government network that is monitored and regularly updated. You should also be familiar with relevant research, documentation, and reporting processes related to security incidents. Desirable certifications include CISSP, GIAC Security+ Intrusion Analyst (GIA), and GIAC Incident Management Consultant (GIAC).

### **SECURITY ANALYST/MANAGER**

Security Analysts protect U.S. Government intelligence data from hackers and other malware. They work to identify weaknesses in the system and develop new strategies. Analysts collect data to spot suspicious activity in databases, server networks, or proprietary software. If a breach happens, they lead the efforts to stop upcoming attacks. Security analysis is an entry-level cybersecurity job that usually requires a degree in Computer Engineering.

### **SECURITY ARCHITECT**

Architects must possess a comprehensive knowledge of the software and systems that protect sensitive data. This includes understanding National Security Network security frameworks, including FedRAMP, NIST, and ISO 27001, hardware configuration, network protocols, and the particular protocols at their employer.

Security Architects need five to ten years of experience, with at least three dedicated to security, before moving into managerial roles in network security. They need to establish familiarity with the systems.

## CLOUD SECURITY SPECIALIST

Cloud Security Specialists manage automated security systems and FedRAMP cloud-based employee information databases. They partner with leaders to set up company policies, cloud network utilization, and customer protection. Most Cloud Security Specialists have at least six to seven years of working with an experienced security professional. Industries that typically use security specialists are aerospace defense contracts, energy and utilities, financials, government, and university education. Cloud Security Specialists need to be up-to-date on FedRAMP cloud requirements.

## PENETRATION TESTER

The role of a **Certified Ethical Hacker (CEH)** is often the most recruited position in Cybersecurity for the Federal Government. Federal agencies, including the CIA, FBI, DHS, NSA, and IRS, will recruit CEHs to help carry out offensive and defensive hacking and counter-hacking operations. This role requires a security clearance.

## SECURITY AUDITOR

Cybersecurity professionals have the potential to advance in security audits. Security Auditors verify safety procedures, secure systems and report on findings. Attention to detail is required when conducting an audit, as vulnerabilities should be identified and addressed promptly. Activities conducted by a Security Auditor include annual penetration testing, documentation, and communication between departments.

# What are the Benefits of Working in Cybersecurity for the Federal Government?

Government work offers job security and superior benefits, which many individuals prefer to the influence of the private sector. The Federal Government also offers competitive salaries as defined under the General Schedule.

## Knowledge for Today and in the Future

The USAJOBS OPM database holds job opportunity announcements (JOAs) for federal roles, including qualifications, duties, salary, duty location, benefits, and security requirements.

The JOA assists applicants in finding the most suitable available job openings by providing a list of frequently used terms that align with their skills, interests, and backgrounds.



# What are the Various Federal Security Clearances?

Security clearances are background checks commonly needed for federal job positions dealing with national security information. This certification process is used to ensure the confidentiality of classified documents.

CIAT.edu highly recommends that students studying the following degrees should invest additional time in learning more about obtaining a clearance:

**Software Development**  
**Cybersecurity**  
**Data Analytics**

Students interested in pursuing federal job positions should be aware of Federal Government and federal contracting employment requirements regarding qualifying for clearance as a condition of employment.

## Road to Your Security Clearance

1

### e-QIP

Applicant fills out security clearance application (e-QIP)

2

### Security Office Review

DCAA security office checks E-QIP for completeness

3

### Background Investigation

DCSA investigates information provided on application

4

### In-person Interview

DCSA investigator may conduct interviews with applicant and coworkers

5

### DCSA Completes Investigation

Report of investigation sent to DODCAF for clearance eligibility

6

### Clearance Award

Applicant notified of results of investigation and clearance awarded

7

### Continuous Vetting

Monitoring of database for changes to credit reports & criminal and public records

# How Important is Security Clearance?

The U.S. Government implements security clearance to protect the country, its citizens, and its allies by restricting access to sensitive information.

- A security clearance is required to gain access to specific classified information.
- To get a security clearance, a Federal Government agency or contractor must employ you, and your role must deem it necessary.
- After securing a role, you may get clearance for the classified material.
- A security clearance is an essential designation within the U.S. National Security System, as it limits access to sensitive information to protect the country and its citizens.

# Why Would an Applicant be Declined for a Clearance?

The Federal Government may refuse an applicant a security clearance because of the results of an investigation, which may include considerations such as honesty, openness, and completion of forms.

- The government investigates the applicant for clearance to ensure that granting or maintaining eligibility for a security clearance aligns with the nation's security interests.
- A security clearance background investigation typically covers personal characteristics, biases, and behavior.
- A sign of issues in these areas may require additional research and result in a clearance denial.

# What are the Various Levels of Security Clearances?

Security clearances have varying levels, each of which requires a background check. Top Secret clearance is the most intensive effort requiring background checks, polygraphs, and interviews.



### Confidential Information

Information requiring security clearance can put national security at risk and must be renewed every 15 years.

### Secret

This security clearance allows access to confidential information that must not be shared without authorized approval. This clearance must be renewed every 10 years.

### Top Secret

This security clearance provides access to critical information for national security information, which must be kept secure. This authorization is valid for five years and must be renewed after that.

The government has various levels of investigation for security clearances that are established depending on the classification and risk associated with the information.

This **table** and list below outline the OPM e-QIP tiers:

#### **TIER 1**

*Low Risk, Non-Sensitive, including HSPD-12 Credentialing, Form SF85.*

#### **TIER 2**

*Moderate Risk Public Trust (MRPT), Form SF85P*

#### **TIER 3**

*Non-Critical Sensitive National Security, Form SF86*

#### **TIER 4**

*High-Risk Public Trust (HRPT), Form SF85P*

#### **TIER 5**

*Critical Sensitive and Special Sensitive National Security, including Top Secret, and SCI, Form SF86*

## What Positions Require a Security Clearance?

Most government departments require employees to have security clearance to perform their jobs. The necessity of requiring a security clearance does not imply a specific position.

Federal Government agencies typically recognize their respective investigations and decisions under reciprocity regulations. Agencies often leverage reciprocity regulations when conducting cross-functional and joint operations.

Agencies needing Top Secret security clearances include the FBI, the Department of Justice, the CIA, the NSA, the DIA, the NRO, and the Department of Homeland Security.

## Who Issues Security Clearances?

The security clearance process involves an applicant submitting forms via the U.S. Office of Personnel Management's e-QIP website, followed by investigations conducted by either the OPM, Department of Defense, Office of Director of National Intelligence, or an Investigation Service Provider (ISP).

While no single Federal Government agency handles all such inquiries, the Department of Defense, Defense Counterintelligence Agencies, and Office of Personnel Management usually manages most of the investigations.

## The Security Clearance Background Investigation Process

To begin the security clearance process, there must be an established requirement for the clearance itself. Organizations with contracts or grants from the Federal Government require their employees to possess a security clearance before employment.

A security clearance is given after the investigation. Individual employees, including newly elected members of Congress, will often be granted an interim Secret or Top Secret security clearance to help fulfill their roles.

The applicant must complete the forms on the OPM website to apply. Afterward, the Department of Defense, Office of National Intelligence, and Office of the Inspector General will begin their investigation.

## Is a Security Clearance Required for Cybersecurity Opportunities?

Security clearances are often needed for personnel working for Federal agencies and their associated contractors.

A security clearance may be required if a person needs to deal with classified information, regardless of the job description.

## Knowledge for Today and in the Future

Security clearances are necessary for protecting against threats originating with hostile intelligence services, cybersecurity threats, terrorists and other threats. This vetting determines who may have access to Government documents or personal information. Equipping yourself with knowledge of security clearances today can help you better navigate the pathways to future careers in the Federal Government.




# What is the Role of a Certified Ethical Hacker in the Federal Government?

---

U.S. Federal Government agencies engage in cyber warfare against malicious hackers who can potentially breach their secure networks, obtain data illegally, and use their computing abilities for pernicious purposes. This form of warfare does not require the use of munitions nor traditional combat or air support; instead, it requires strategic espionage, covert operations, and a team of specialists known as **Certified Ethical Hackers (CEH)**.

Students looking to become Certified Ethical Hackers (CEH) are recommended to review the advanced certification programs offered by CIAT.edu. The San Diego-based education institution offers several cybersecurity degree programs and certifications:

-  **Certified Ethical Hacker (CEH) Certification**
-  **CISSP Certification**
-  **CompTIA Security+ Certification**
-  **Applied Bachelor's Degree in Computer Information Systems – Cybersecurity Concentration**

This section will discuss various requirements for students seeking a career as a U.S. Government certified hacker. We will discuss the education requirements,

DoD credential requirements, and certification required for this exciting career opportunity.

Students could consider many career paths when applying for the Federal cybersecurity workforce. Federal agencies continue to compete with the private industry for talent. The field of Cybersecurity continues to have one of the lowest unemployment rates in the world. Students with industry certifications and hacking experience are in demand by Federal agencies.

## Can you Work as a Hacker for the Government?

The U.S. federal government is engaging in cyber warfare to combat those who infiltrate secure networks, commit data theft, and use their computer skills for malicious activities.

According to projections, global cybercrime costs are expected to reach \$6 trillion annually by 2021. To prevent such crimes, ethical hacking is seen as one of the critical strategies. It involves disrupting malicious activities, identifying target points and tactics, and opposing attackers' actions.

The government constantly recruits certified ethical hackers (CEH) to become cyber warriors fighting against state-sponsored hackers from China, Russia, North Korea, and other countries.

## What are the Requirements for Becoming a Hacker for the Federal Government?

The Department of Defense (DoD) recently changed the 8570 Directive, the Information Assurance Workforce Improvement Program, to the 8140 Directive, which necessitates certifications for DoD employees and contractors in their respective areas of professional specialization.

Government agencies require professionals to fulfill specific certification requirements to ensure competency and ethical practices in cybersecurity. These certifications are necessary to detect weaknesses in IT systems using malicious attack techniques.

The Certified Ethical Hacker (CEH) course is created to fulfill the requirements of DoD 8570 and DoD 8410. It covers topics related to cyber threats, such as



information security, vulnerability management, network enumeration, etc. The aim is to validate the participant's knowledge regarding the country's national security.

## Origins of Ethical Hacking

Hack activities originated at Boston University in the 1960s, where they were positively perceived as creative techniques for using machine tools. By the mid-1990s, malicious hacking had increased due to expanded consumer computer use.

Today, ethical hacking has become essential for companies and governments to protect assets and people from bad actors. Organizations clearly understand cybersecurity risks by hiring hackers for their internal and external systems.

Overall, hackers usually fall into one of three categories:

### The White-Hat Hacker

Their purpose is to find and identify potential vulnerabilities so that countermeasures can be taken to protect the system.

### The Gray-Hat Hackers

Gray-Hat hacking engagements are more collaborative than others. In this engagement, the various agencies will share login information with the penetration testers and goals to validate their current security posture.

### The Black-Hat Hackers

Black-hat hackers are notorious for breaching networks to threaten victims by disrupting or destroying data, conducting espionage, and committing malicious acts.

## Skills and Certifications Required for Ethical Hackers

An ethical hacking job typically requires a technology or computer science bachelor's degree. If a degree is absent, experience and certifications are used by employers to assess candidates.

Applicants looking to secure a federal government position involving national cybersecurity activities should look into obtaining the **Certified Ethical Hacking Certification**. This certification will help satisfy specific requirements outlined by the DoD 8570 and DoD 8410 standards as mandated by the U.S. Department of Defense; [CIAT.edu](https://www.ciat.edu) provides a **course** to equip students with this certification.



# Managing Secured Data for the Federal Government

---

Protecting the data of the United States Government is a multi-layer process that involves multiple departments and deeply-divided containerization of content. The Federal Government and associated defense contractors struggled for years to meet compliance requirements for contracting; many firms turned their attention away from the Federal Government.

The security of information technology systems and data is essential for the successful functioning of Federal agencies and critical infrastructures such as energy, transportation, communications, and financial services.

Students studying for a degree in Software Development, Data Analytics, or Cybersecurity at [CIAT.edu](https://www.ciat.edu) that plan to apply for jobs in the Federal Information Systems groups should continue to research the various data security frameworks and compliance regulations for protecting the U.S. government.

This section discusses the various Federal departments, including the Department of Homeland Security and the Department of Defense; civilian agencies, including the National Security Agency, the Central Intelligence Agency, and the Federal Bureau of Investigation; and how these departments and agencies leverage compliance frameworks, data sharing, and data classification strategies.

# Navigating Federal Compliance Requirements

Thanks partly to new Federal Government frameworks and initiatives to promote security and collaboration, data protection has become manageable—but it could be better. Good protection ensures public trust and strengthens national security, economic growth, and well-being.

Most existing federal government systems and processes in the last century provide data or statistics regularly; however, today's needs demand insights within days or hours. These legacy systems could have done more to promote data sharing or collaboration. Many departments purposely isolated themselves from each to protect their data and funding sources.

The current federal government data system is transforming, promoting collaboration and sharing. With a coordinated strategy, decision-makers at all levels of government need to protect their data and help restrict access to adjacent departments. Although decentralization supports decision-makers' interests, its limits hinder data sharing, resulting in initiatives like the Cyber Information Sharing and Collaboration Program (CISCP).

## What is the CISCP Program?

"The Cyber Information Sharing and Collaboration Program (CISCP) promotes sharing cyber threats, incidents, and vulnerability data." Through CISA Central (formerly the National Cybersecurity and Communications Integration Center (NCCIC)), members can gain greater insight into security risks and develop more effective countermeasures.

## What is CISA?

The Cybersecurity and Infrastructure Security Agency (CISA) collaborates with federal civilian departments and agencies to implement risk-minded policies and procedures to stay ahead of advancing risks. CISA distributes automated alerts in both the public and private sectors to fortify cyber networks. This method structures cybersecurity endeavors by providing assets that can be tapped into quickly, effectively carrying out prescribed protection methods.

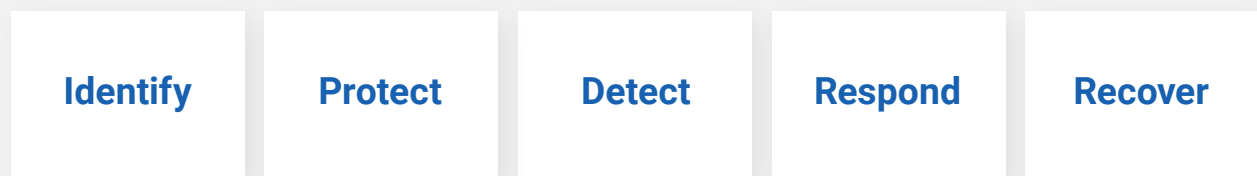
CISA and other federal agencies invest considerable funds in creating cybersecurity and risk management frameworks to help the public and U.S. companies stay secure. For example, CISA provides recovery support functions for ransomware attacks and insight into threat intelligence information documenting future foreseeable risks. Moreover, the agency also provides frameworks to help hire cybersecurity talent and provides a foundation for information sharing and collaboration.

To move forward, the federal government requires a Digital Strategy that uses fewer resources and facilitates innovation while utilizing government data to serve Americans better. With the establishment of the Cybersecurity and Infrastructure Agency (CISA), the inception of the National Institute of Standards and Technology (NIST) 800 series framework, and the guidelines for assisting employers in hiring cybersecurity talent, these government initiatives continue to help protect sensitive and secure data.

## Understand the Importance of NIST-800-53

### NIST-800-53 FRAMEWORKS

NIST Cybersecurity Framework (CSF) is a set of guidelines and principles organizations should follow to address cybersecurity risks. NIST SP 800-53 also introduces the security control baselines. NIST contains five focus areas:



Federal government agencies and non-government organizations use NIST-800-53 to comply with multiple regulatory standards and also reduce the potential risk of external threats from terrorist groups, state-sponsored cyber terrorism, and domestic cyber incidents from within the United States.

Before NIST-800, several government agencies developed their security standards and policies. NIST created a set of industry frameworks, architectures, and procedures designed to meet these regulatory mandates and defend against

cybersecurity events against critical infrastructure services. Using NIST-800-53, organizations can simplify their governance needs for various regulations such as PCI-DSS, HIPAA, and CCPA.

## Why is NIST-800-53 Critical to the Federal Government?

NIST SP 500-53 delivers a unified information security framework and enterprise risk management program for agencies and defense contractors to align to. The United States government leverages NIST for all departments to have a common and effective risk management framework, excluding agencies that deal with national security. Those departments align more with the FedRAMP framework for cloud security.

Compliance with NIST SP 800-53 and other NIST guidelines is significant in FISMA and FedRAMP compliance. This framework helps improve the security rating of your organization by providing a secure foundation for information systems, industry best-practice around incident response practices, and standards for encryption measures.

Complying with NIST SP 800-53 and other standards helps organizations improve their compliance with data protection laws and regulations such as the SHIELD Act, LGPD, GDPR, CCPA, GLBA, PIPEDA, HIPAA, PCI DSS, and 23 NYCRR 500.

For effective data collaboration, it is imperative to understand the importance of protecting critical and secretive U.S. government data and data classification.

## Federal Government Standards and Mandates for Data Protection and Classification

Data classification is a process used in information security that involves assigning a sensitivity level to data and determining the baseline security controls to protect it from unauthorized disclosure, alteration, or destruction.

# Knowledge for Today and in the Future

CIAT.Edu provides ideal Degree and Certification Programs that align with a future career in the federal government. Explore these program paths below:

-  **Applied Bachelor's Degree in Computer Information Systems–Cybersecurity Concentration**
-  **Certified Ethical Hacker (CEH) Certification–CEH–V11**
-  **CISSP Certification**
-  **AWS Security Specialty Certification**





# What is FedRAMP?

---

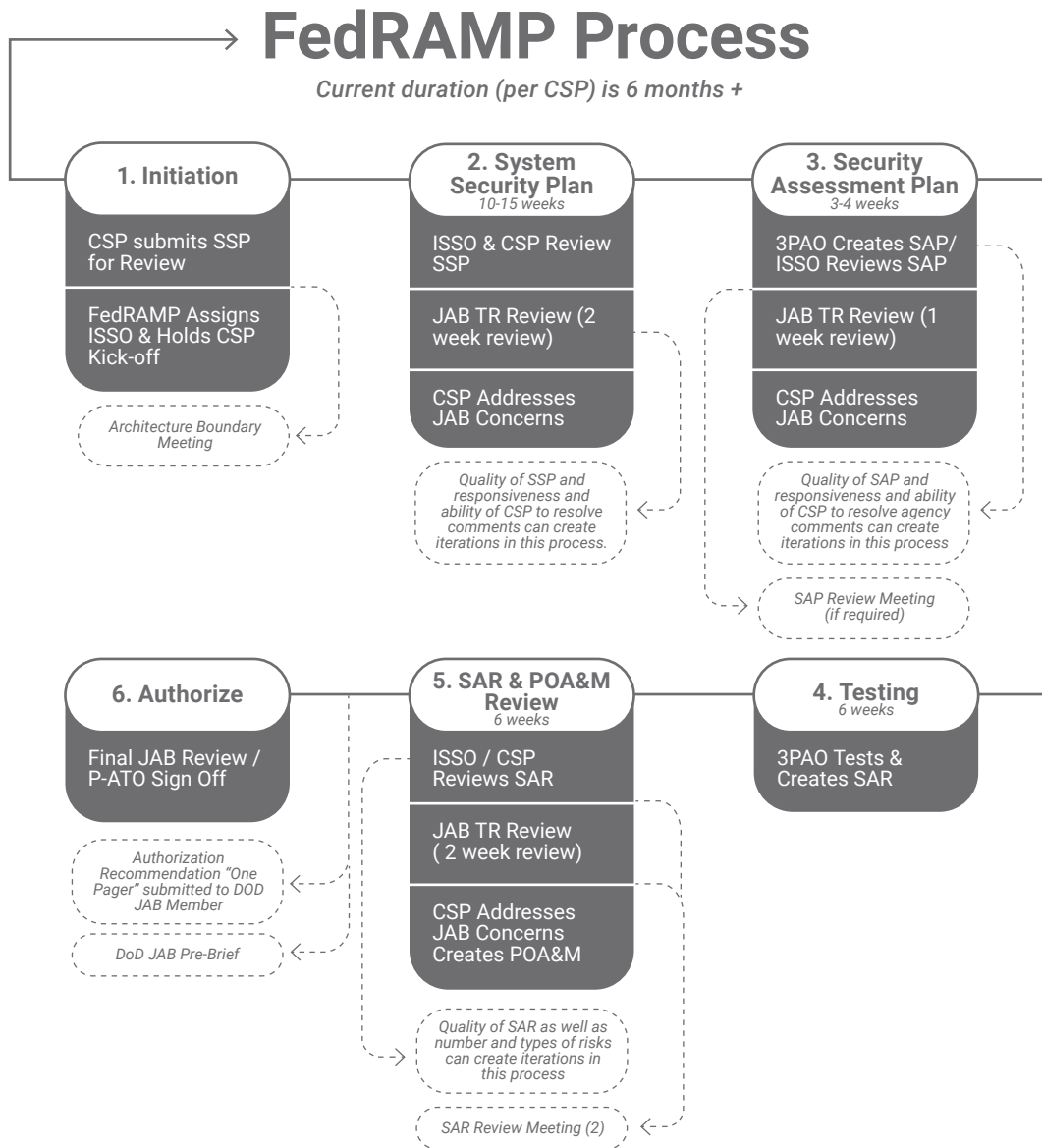
The Federal Risk and Authorization Management Program (FedRAMP) is a compliance framework established by the US government, which details requirements for cloud services offering and requirements for approved cloud service offerings for Federal Government Agencies. FedRAMP-compliant mandates strict compliance for cloud products and services regarding their authorization, security assessment, and continuous monitoring approach to their respective offerings.

Students pursuing a degree in **Cybersecurity** and a **CISSP** certification from **CIAT.edu** should continue researching the FedRAMP requirement for cloud providers.

This San Diego-based education institution offers several programs to assist students with the knowledge in pursuing a career in Federal Government Security and Cloud Technology, including:

-  **Applied Bachelor's Degree in Computer Information Systems – Cybersecurity Concentration**
-  **Associate of Applied Science in Software Development**
-  **AWS Security Specialty Certification**
-  **Applied Bachelor's Degree in Computer Information Systems – Cloud Concentration**

This section will discuss the need for FedRAMP, which **cloud** providers are FedRAMP certified, and what steps these providers need to take to become FedRAMP-approved and authorized.



## Why is FedRAMP Important?

The Federal Government developed FedRAMP to provide a standardized approach with enhanced transparency, including completing a security assessment of agreed-upon standards, documentation of the current security posture, and continuous monitoring for cloud products and services used by Federal entities. This mandate supported the Federal Government’s ‘cloud first’ initiative by allowing agencies to contract with approved cloud providers to

best secure government information. All approved cloud providers that meet FedRAMP standards become listed in the FedRAMP marketplace.

In 2011, the FedRAMP security assessment framework offered a cost-efficient and risk-sensitive approach to cloud adoption for Federal Government Agencies. Its development drew upon the Risk Management Framework (RMF) consistent with FISMA (Federal Information Security Modernization Act) regulations and NIST SP 800-53. Through FedRAMP, cloud service providers (CSPs) can get assessments and authorizations from federal agencies.

The goal of FedRAMP, as stated by the U.S. General Services Administration (GSA), is to improve the adoption of cloud computing through reusable assessments and a rigorous authorization process in compliance with extensive security control requirements. Achieving FedRAMP authorization will provide further assurance of the security and effectiveness of cloud solutions for organizations. Becoming FedRAMP authorized is both a business and technical achievement for cloud service providers.

## Why is FedRAMP Authorization Valuable to Cloud Service Providers (CSPs)?

Cloud providers, including Amazon Web Services, Google, Microsoft, IBM, and Blackberry, all hold FedRAMP certifications. Chief Information Officers focusing on digital transformation supporting their Federal Government customers must ensure their cloud provider complies with FedRAMP.

Being FedRAMP authorized is critical for cloud providers wanting to capture Federal business. Many DoD, Federal departments, and civilian agencies still run legacy applications within their data centers. Moving to the cloud is less likely to happen if it jeopardizes U.S. secret or top-secret data.

## FedRAMP Authorization Process

Cloud service providers who want to provide products and services to the US government must have FedRAMP compliance. The cloud providers must follow the NIST-800 series framework and Federal Information Security Management Act (FISMA). Cloud providers must adhere to the FedRAMP framework, including

hiring an approved FedRAMP third-party assessment organization (3PAO) and assessment firm to receive the authority to operate as a FedRAMP Secure cloud offering.

Third-party assessment organizations (3PAO) are integral to the FedRAMP security assessment process. Their domain expertise around FedRAMP security requirements, modern cloud technologies, and FedRAMP's continuous operations models is essential for cloud providers looking to meet Federal Cybersecurity requirements for their secure cloud products.

FedRAMP 3PAO organizations are accredited by the American Association for Laboratory Accreditation (A2LA) and must exhibit independence and a technical understanding to assess security implementations and produce evidence. These auditors validate that the cloud providers have deployed, updated, and monitored all essential FedRAMP controls to become FedRAMP authorized. Various government agencies require 3PAO assessments across agencies that plan to share data with their respective government entities.

## Knowledge for Today and in the Future

All prospective employers of the Defense Industrial Base (DIB), all Federal agencies, departments, and the military must work with a FedRAMP-certified cloud provider if they plan to migrate or access data from the cloud. Students applying for a software development, **cloud engineering**, and cybersecurity role should expand their knowledge base by reading and by watching YouTube videos discussing the importance of FedRAMP and its role in protecting U.S. Government data.



# What are the Implications of CMMC in 2023?

---

The Cybersecurity Maturity Model Certification (CMMC 2.0) will be mandatory for defense contractors and subcontractors starting in 2024. Once CMMC 2.0 becomes implemented, organizations can determine whether they're eligible for government contracts by meeting these compliance requirements to achieve the proper certification levels.

Students should invest time in online learning, attend seminars around NIST 800-171 and CMMC 2.0 compliance, and watch YouTube videos about this fantastic subject.

## Purpose of CMMC?

CMMC ensured the safety and accountability of companies to meet DoD assessment requirements of the sensitive information exchanged between the U.S. Department of Defence (DoD) and the contractors who supply them. CMMC ensures DoD shares only secure information with these companies that align with 800-171 compliance security controls. Foreign nationals, state-sponsored cybercriminals, and global terrorist organizations constantly attack the defense industry. CMMC is essential for defense industrial contractors to comply with combating these complex cyberattacks to prevent important national security data from falling into the wrong hands.

CMMC 2.0 also certifies the security measures taken by those companies to make sure they meet the highest standards to handle complex cyber-attacks by

deploying, monitoring, and maintaining a strict security framework. The primary goal of CMMC is to ensure that the organizations they work with are safe from hackers while maintaining an agile security program.

## How is CMMC Different from NIST 800-171?

The most significant difference between CMMC and traditional security testing is that CMMC uses an assessment method called a “maturing” approach. It’s like a certification program, but you pass through each stage instead of passing exams by demonstrating competency.

NIST 800–171 (the U.S. government’s cybersecurity standards) and CMMC (a European Union initiative for cyber risk management) are different security control frameworks. Still, the new CMCC 2 framework became inspired by them.

## How Long Does CMMC Certification Take?

The process can take months. Organizations must engage outside firms to validate their approach to align with the CMMC regulatory requirements.

## What Does This Mean for Your Government Contracts?

CMMC 2.2 requires contractors to comply with cybersecurity requirements and specific standards related to their business models. These firms must show their cyber hygiene practices through third-party risk audits to meet CMMC 2.0 certification requirements. Without CMMC 2.0 certifications, defense contractors cannot bid or conduct business with the federal government or military.

## Begin with the Evaluating your Internal Resources to Support CMMC

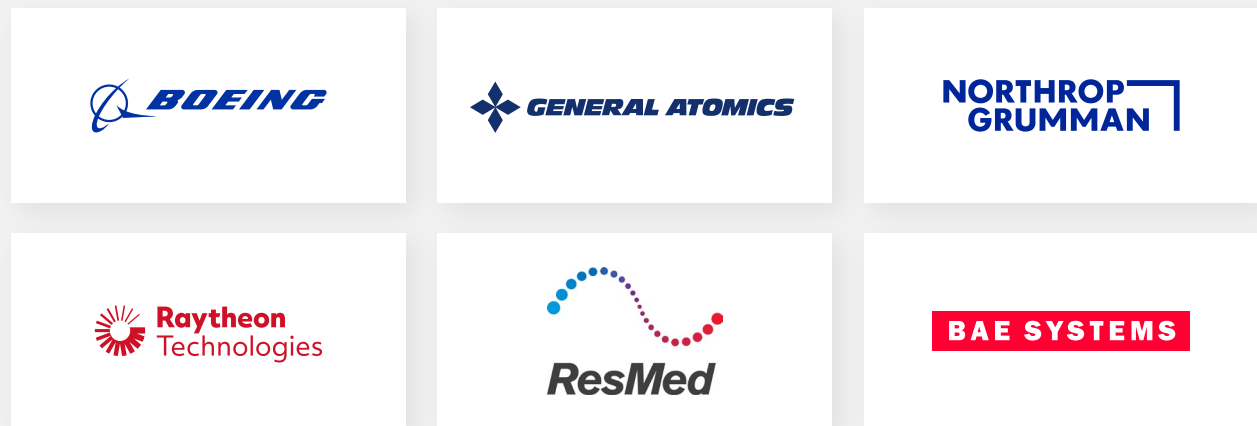
Can CMMCs fulfill their targets and meet their needs? How does the CMMC change the way the organization operates? Do we still need internal resources for the proper certifications and ongoing maintenance?



Supporting CMMC and NIST 800-171 requires experienced compliance, risk, and cybersecurity resources to coordinate and collaborate to maintain this credential. Organizations also could leverage managed security service providers (MSSP) for help in monitoring, incident response, and SecOps to help augment with experienced resources.

## Knowledge for Today and in the Future

Many IT and cybersecurity professionals should continue investing time into learning more about NIST-800 and CMMC compliance mandates coming in 2023 and 2024. Many employers conducting business with the federal government will need a CMMC level 2 or 3 in 2023 to qualify to bid on contracts. An example of these employers include:



Organizations continue the challenge globally to find qualified compliance and cybersecurity talent. CIAT offers three learning paths, from certificate to degree-level programs dedicated to cybersecurity and compliance, to help military and non-military individuals access these in-demand positions.



# Take the First Step

---

## **REAL-WORLD PREPARATION AT CIAT.EDU**

CIAT is a military-friendly school, and you deserve an education worthy of your service. We offer twelve programs for active duty members and veterans, along with a combination of certifications and hands-on training that empower you to take your education to the next level. Whether advancing your career in the armed forces or transitioning back into civilian life, CIAT will ensure you're prepared for everything.

## **MOST MILITARY-SUPPORTIVE COLLEGES IN THE VA PACIFIC DISTRICT**

CIAT has been included in the Editor's Choice for 2022: Top Picks for the Most Military-Supportive Colleges and Universities in the Western U.S. and ranked as one of the "The Most Military-Supportive Colleges in the VA Pacific District". Yellow Ribbon is a joint VA/college program where each participating school agrees to kick in a set amount of tuition coverage for a set number of students who don't have their tuition costs wholly covered by GI Bill® benefits.

**CIAT delivers practical, hands-on, and theoretical training** for a comprehensive education that empowers and prepares you to take on the world. Here are some resources we offer to get you there:

- Hands-on physical labs kits paired with virtual learning activities
- Software access for certification exam preparation and coding development environments
- Interactive live lectures from certified instructors
- Personalized career coaching and job placement support

The Cybersecurity industry encourages students seeking a career in cybersecurity in the Federal Government are encouraged to look into courses and certifications offered at CIAT.edu:

-  **Applied for Bachelor's Degree in Computer Information Systems–Cybersecurity Concentration**
-  **CISSP Certification**
-  **CompTIA Security+ Certification**
-  **Certified Ethical Hacker (CEH) Certification–CEH–V11**
-  **AWS Security Specialty Certification**

CIAT.edu offers several degree programs in cybersecurity and IT certifications if students want to learn about penetration testing, red team, blue team engagements, and application testing.

CIAT offers a unique spin on what we have traditionally expected of a four-year degree. CIAT students earn in-demand industry IT certifications with each set of technical courses, and graduates complete their programs positioned to compete for in-demand technology jobs.

### **ACTIVE DUTY TUITION ASSISTANCE**

At CIAT, we know how difficult it can be juggling active duty while expanding your education. How could you squeeze in classes and studying while on-call and ready for deployment 24/7? That's where we can help. Our flexible in-person and online course schedules make it easy to earn your degree no matter where you're stationed. CIAT also offers **Active Duty Tuition Assistance** to help pay your new degree bill. Tuition Assistance (TA) funds are a unique, distinct source of financial aid available to eligible Service members. Tuition Assistance (TA) will be classified as a "first payer" and be applied to students' accounts before the application of any Pell Grant awarded.

## **Let Us Help You Achieve Your Career Goals**

When landing your dream job, CIAT supports its students every step of the way—ensuring you graduate with more than just a degree. Our IT career coaching services focus on professional and personal development to help prepare you for your career.

[\*\*Request Support Today To Get Started\*\*](#)