The [United States Military Academy](https://www.westpoint.edu/about/west-point-staff/chief-information-officer-G6) (USMA) is accepting applications for the position of Chief

Information Security Officer (CISO). The Academy is the Army’s premier leadership institution with 4,400 undergraduate-only students, 2,500 faculty and staff, and also directly supports the USMA Preparatory School (USMAPS) of 200 cadet candidates and 70 staff and faculty. The Academy is located 50 miles north of New York City, in the scenic Hudson Valley.

The CISO oversees strategy, operations, and the budget for the protection of the Academy’s information, information systems, and related assets and manages that protection program. The scope of responsibility encompasses leadership, communications, applications, infrastructure, policies and procedures which apply for higher educational institutions, federal entities, Department of the Army, and Department of Defense organizations.

The CISO is an administrative Title 10 faculty position that includes teaching, as duties permit, and as approved by the USMA Chief Information Officer (CIO)/G6. USMA Tenure-Track or Tenured faculty members assigned to this administrative position retain their Tenure-Track or Tenured status. The CISO will be appointed to both the USMA Staff CIO/G6 directorate and, in coordination with the Dean of the Academic Board, an [academic department](https://www.westpoint.edu/academics/academic-departments)’s teaching faculty. In order to teach, an academic department will vet the CISO through their Faculty Development Workshop (FDW). The CISO’s teaching load will be a maximum of one course section (12-18 students), in-person, annually.

Serving as the CISO under the [USMA CIO](https://www.westpoint.edu/about/west-point-staff/chief-information-officer-G6), the incumbent advises on all matters relating to Cybersecurity. As the director of the USMA Cybersecurity branch, the CISO works closely with the USMA IT Strategy Committee, Army Cyber Command, Army’s Network Enterprise Technology Command (NETCOM), the Department of the Army Headquarters G6 Staff, the Assistant Secretary of the Army CIO staff and other external entities on all Cybersecurity matters. The CISO also maintains relationships with colleagues at other federal service academies and higher educational programs, institutions, and professional forums (e.g., [EDUCAUSE](https://www.educause.edu/), [NYSERNET](https://www.nysernet.org/)). The CISO, also appointed as the Program Information System Security Manager (P-ISSM), represents USMA and USMA interests at all Army-wide P-ISSM events and forums. It is essential that the CISO sustain USMA leadership’s freedom of action through relationship building, maintenance, and transparency. Presently, P-ISSM representation remains primarily remote while CISO duties remain primarily in-person/on-premise.

Title 10 pay tables at USMA are not publicly available, but there is [good background reading](https://www.federalpay.org/articles/civilian-faculty-pay-schedule) and the [US Naval Academy’s pay scales](https://www.usna.edu/HRO/_files/documents/Faculty_Pay_Table_2022.pdf) are comparable. The range at USMA is from $100,000-$175,000. Moving expenses are negotiable.

Other tasks include:

* Manage and curate the USMA Authority to Operate via the Risk Management Framework using NIST 800-53 in support of the USMA Mission
* Lead the Cybersecurity branch of the CISO with a 10 direct reports and 85 indirect reports from across the Academy. Presently, the direct reports are a mix of on-premise and remote workforce, while the 85 indirect reports work, primarily, on-premise.
* Advise and assist in the implementation of system security designs of the campus infrastructure, as well as systems and capabilities requested, developed, purchased, and otherwise in use by the Academy’s stakeholders
* Ensure that disaster recovery and business continuity plans are in place and tested regularly
* Review and advise the creation and modification of security policies, controls and assessment procedures
* Review and advise senior leadership of the creation and modification cyber incident response plans, rehearsals, execution, and lessons learned
* Lead and review investigations after breaches or incidents, including impact analysis and recommendations for avoiding similar breaches or incidents
* Update the current understanding of the threat landscape to maintain or evolve an appropriate cyber posture
* Advise and assist USMA entities on compliance with policies and regulations (e.g., Privacy Act, Freedom of Information Act, Federal Information Systems Management Act (FISMA), Office of Management and Budget (OMB) Systems of Record registrations and notices).
* Incorporate policies and regulations to identify risks and actionable plans enabling the USMA mission and a suitable enterprise cyber-defensive posture
* Schedule and conduct periodic security audits and assessments, including table top exercises
* Enable enterprise-wide education with respect to cybersecurity practices, policies, and procedures and ensure compliance is enforced
* Provide training and mentoring to cyber team members and the USMA IT workforce

Applicants must have a strong commitment to the educational, military, physical, and character development of cadets. Applicants should be experienced in Cybersecurity processes, regulations and best practices, enterprise IT architecture, client IT services, and Army and DoD IT management organizations and processes. A current certification compliant with DoD 8570.01M for Information Assurance Management III (IAM III) is mandatory and a minimum of a MS in a closely associated field is necessary to be a faculty member.. IAM III certifications include: Certified Information Systems Manager (CISM), Certified Information Systems Security Professional (CISSP), GIAC Security Leadership (GSLC), and Certified CISO (CCISO).

Applicants should also possess significant leadership experience, completion of advanced degree(s) and certification(s), and recent experience as a CISO or related position(s) in higher education. Applicants should contact: Ms. Angie Mathews (angie.mathews@westpoint.edu). Completed applications must be received by (xx\_To Be Determined\_xx once the Academy posts the announcement on [USAJobs.gov](https://www.usajobs.gov/)). The United States Military Academy is an Equal Opportunity, Affirmative Action Employer. Women and minorities are encouraged to apply.

Specialized Skills:

* Experience implementing NIST Risk Management Framework at a higher educational institution(s) inclusive of guest user and bring your own device (BYOD) environments, congressional delegation support, annual applicant pools exceeding 15,000 persons, college business operations, educational activities of 13 academic departments with over 40 degree programs, and research by staff and faculty across 30 different research centers.
* Experience with hybrid environments of on-premises computing and 40+ cloud vendor computing resources (e.g., Student Information Systems, Learning Management Systems, Student Athlete Wellness/Performance tracking systems, educational material delivery and grading). Devices include 400+ real and virtual servers, 10,000+ end point computers (managed and unmanaged), laboratory and research systems, ICS/SCADA systems, PCI systems, 8,000+ mobile devices (e.g., phones, tablets), 3,000+ gaming and personal computing systems, 2,800+ Wireless Access Points.
* Experience navigating bureaucracies and governance processes to enable and sustain freedom of action and decision making for a minority position within much larger organizations.
* Experience building coalitions of organizations to gain leverage and strength of argument to enable and sustain freedom of action and decision making
* Experience leading small teams and development of automation to manage cybersecurity operations (e.g., SIEM/SOAR tools [e.g., Azure Sentinel, Splunk], vulnerability scanning/scanners, automated security checks), forensic and incident response tools and automation, support various forms of fact findings, and as necessary, law enforcement). Experience moving organizations and processes from manual and point-in-time evaluations to continuous monitoring and reporting via automation.
* Experience configuring, operating, and defending Office 365 Enterprise/Academic tenants and those tenant’s in-built security capabilities, current Windows client and server builds and management at the enterprise level, and use of MS Defender Enterprise Management.
* Experience advising and coordinating integration of Identity Management (e.g., Azure Active Directory and Active Directory), Device Health and Management (e.g., MS Endpoint Manager (formerly MS InTune), Cisco Identity Services Engine (ISE)), Network Access (Cisco ISE, 802.1x), macro and micro-network segmentation, conditional access policies, and other technologies and capabilities in support of USMA’s Implementation of Zero Trust Architecture and Executive Order 14208. Working knowledge of incorporating and defending Linux and Mac platforms into a heterogenous environment as well as supporting on-network Internet of Things use while maintaining security of USMA’s information and IT systems.
* Pass a National Agency Check with Inquiries (NACI) security background check
* Gain and maintain a US Government Secret security clearance

The Official Job Announcement will be on <https://www.usajobs.gov/> no later than end of February 2022.