STATE OF IDAHO
invites applications for the position of:

IOEM Cybersecurity Program Manager and Critical Infrastructure Key Resources (CIKR) Planner

SALARY:	$31.08 - $40.41 Hourly
DEPARTMENT:	Division of Military
OPENING DATE:	12/16/21
CLOSING DATE:	01/17/22 11:59 PM
DESCRIPTION:	

STATE OF IDAHO
MILITARY DIVISION
Human Resource Office (HRO)
State Personnel Branch
4794 General Manning Avenue, Building 442
Boise, ID 83705-8112
Telephone: (208) 801-4273

STATE VACANCY ANNOUNCEMENT
Registers established from this announcement may remain valid up to one year to fill vacancies.

ANNOUNCEMENT NUMBER:	**21-105-N**
AREA OF CONSIDERATION:	**Open to all applicants**
POSITION TITLE:	**IOEM Cybersecurity Program Manager and Critical Infrastructure Key Resources (CIKR) Planner**
PAY GRADE:	**NGA-11**
POSITION CONTROL NUMBER:	**6038**
CLASS CODE:	**22708**
SALARY:	**$31.08 to $40.41 hourly ($64,649 to $84,049 annually)**
FLSA CODE:	**Administrative Exempt**
DUTY LOCATION:	**Military Division, Idaho Office of Emergency Management (IOEM), Gowen Field, Boise, ID**
TYPE OF POSITION:	**Civilian Nonclassified; Limited Service Appointment** *(This position is under a cooperative agreement or grant funded.)*
COMPATIBLE MILITARY FIELD:	**Not Applicable**

JOB TITLE: IOEM CYBERSECURITY PROGRAM MANAGER AND CRITICAL INFRASTRUCTURE KEY RESOURCES (CIKR) PLANNER
POSITION CONTROL NUMBER: 6038
CLASS CODE NUMBER: 22708
SALARY GRADE: NGA-11

INTRODUCTION: This position is assigned to the Preparedness and Protection Branch of the Idaho Office of Emergency Management (IOEM), functioning within the State of Idaho – Military Division. The primary purpose of this position is to manage the IOEM Cybersecurity Program. Coordinates with public, private and non-profit sectors, and every level of government to report, prevent, respond to, mitigate, and recover from state emergency level cyber security incidents and disaster events. This position will also develop, implement and maintain Critical Infrastructure/Key Resource (CI/KR) Protection Program as a component of the state's overarching Homeland Security Program. Supports IOEMs responsibility to coordinate state and federal emergency response, recovery and mitigation operations during emergencies and disasters; as well as develop and coordinate the preparation and implementation of plans and programs for prevention, protection and mitigation to reduce the harmful consequences of disasters.

EXAMPLE OF DUTIES:

DUTIES AND RESPONSIBILITIES:

1. **Cyber Response Process:** Responsible for being a liaison for emergency management during the Idaho Office of Information Technology Services (ITS) administration of the Cyber Incident Response process. Ensures proper preparedness and coordination across governmental and private sectors. Coordinates through ITS to help assess and measure cascading impacts that might arise from cyber incidents across emergency management sectors.

2. **Maintain State Cyber Plan:** Develops, coordinates, and maintains the State of Idaho Cyber Incident Response Plan (Incident Annex #7) to the State of Idaho Emergency Operations Plan (IDEOP). Integrates cyber planning processes into all phases of Emergency Management planning across the State of Idaho. Works with city, county and tribal emergency managers to integrate cyber security strategies as part of their emergency management processes. Coordinate with Governor's appointed Homeland Security Advisor (HSA), as well as the Federal Emergency Management Agency (FEMA) and the Department of Homeland Security (DHS) on all state emergency and disaster related cyber related issues including intrusions, grant funding and project eligibility.

3. **Cyber Training & Exercise:** Develops and coordinates statewide cyber exercises, training, and plans that address response, prevention, mitigation, and recovery related to state emergency and disaster related cyber incidents. Coordinates the development of cyber security training opportunities for State and local governments, tribes and businesses in Idaho within the scope of IOEM. Works across functional units within the Idaho Military Division (IMD) and IOEM to integrate cyber planning into other planning and exercise processes. Coordinates with the IOEM Training & Exercise section. Facilitates the development, planning, and coordination of recurring emergency and disaster related cyber exercises with the Governor's appointed Homeland Security Advisor (HSA), the Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA). Supports the HSA for Training and Exercise (T&E), planning, prevention, protection, mitigation and response efforts related to emergency and disaster related cybersecurity. Serves as the IOEM lead and coordinates with the ITS Chief Information Security Officer as needed.

4. **Grants and Reports:** Develops, manages and submits Homeland Security Grant applications for cyber resources within the State of Idaho. Designs, coordinates, and develops annual Homeland Security grant submissions and reports for cyber security initiatives.

5. **Coordination:** Functions as the IOEM official representative for any workgroup concerned with cyber capabilities and response planning efforts including multi-state committees or government led cyber security work groups.

6. **Cyber Security Events:** Serves as the primary IOEM representative to the Idaho State Fusion Center for cyber incident matters. Coordinates with Information Technology Services (ITS) and the Idaho Fusion Center on cyber security issues that impact the State of Idaho. Serves as the IOEM lead for coordinating significant cyber security matters with state, federal, local, tribal, and private sector. Develops and distributes support and request templates to facilitate information flow during a significant cyber event. Develops and maintains information sharing relationships and liaison with the Office of the Chief Information Officer, Department of Administration and the Idaho State Police.

7. **Cyber CIKR Critical Infrastructure:** Develops and maintains current contact lists of cyber and CIKR Point of Contacts (POCs) representing each of the 16 Critical Infrastructure/Key Resource (CIKR) sectors throughout the State of Idaho. Works to develop appropriately protected priority asset lists to facilitate significant cyber/CIKR response activities. Develops and maintains contact lists of cyber security resource types at the state and national level to assist and advise when there are questions or issues.

8. Develops project plans with a scope of work and budget that meets stated goals and objectives; plans, coordinates and implements program activities; evaluates programs effectiveness, identifies problems and recommends changes; coordinates budget needs; monitors budget and expenditures against program progress; reviews and approves projects, monitors progress reports for eligible reimbursement requests, adherence to scope of work, and provides assistance for corrective measures. Develops, implements and maintains a critical knowledge base and plans for infrastructure protection. Develops a collaborative partnership between and among a diverse set of security partners including federal, state, local and tribal governments, and private industry.

9. On a voluntary basis, attends training and performs duties as the on-call IOEM HAZMAT Duty Officer several times per year, on a 24/7 weekly basis, in accordance with established rotation schedule.

10. Performs other related duties and projects as necessary or assigned. Deploys as directed to a designated Emergency Operations Center at a local, state, or federal level during federally declared disasters. Upon activation of the Idaho State Emergency Operations Center (IDEOC), performs duties as directed by the IDEOC Manager. During activation of the IOEM's Continuity of Operations (COOP) Plan, may perform as member of Advance Echelon party (ADVON) and/or other supporting COOP role as required.

SUPERVISORY CONTROLS: Duties are performed under the general supervision of the IOEM Preparedness and Protection Branch Chief. The incumbent receives broadly defined strategic and tactical assignments that support the overall mission goals. The incumbent works independently to define overall project objectives, schedule and cost estimates to fulfill assignments. Sets priorities within general guidelines and as coordinated. Works collaboratively with federal, state and local officials. Keeps supervisor informed of work progress, factors that may influence the success of assignments, and potentially controversial matters. Carries out work using applicable regulations, policies and directives.

PERSONAL WORK CONTACTS: Contacts include IOEM Management and staff; Idaho National Guard Commanders and staff; city, county, state, and federal employees from various agencies; and leaders in private industry. Private sector owners and operators of critical infrastructure/key resources companies will be the primary focus of the incumbent's day-to-day responsibilities.

WORKING CONDITIONS / PHYSICAL EFFORT: The majority of work is performed in an office environment. Work may require travel and outdoor exposure in all types of weather. Field activities may require incumbent to travel and work long hours; driving and walking over rough, uneven surfaces; standing, stooping, reaching; and occasional lifting of moderately heavy items such as equipment or supplies up to 50 pounds. Working around damaged facilities and structures can be very hazardous. Incumbent is required to deploy to the field upon request of the immediate supervisor or the IOEM Director. During emergencies and disasters, the incumbent may be required to deal with citizens, government officials, and/or organizations under emotional distress because of the loss of lives and personal property. Moderate travel, in and outside of the State of Idaho, is required. International travel may be required. Promotes a

respectful workplace that complies with policies of the Adjutant General. Observes and ensures compliance with all applicable laws, rules, regulations and policies and serves as a role model for the Whistleblower Protection Program, EEO, security and workplace safety practices, policies and regulations at all times. Maintains a safe and drug/alcohol free workplace.

FLSA Overtime Code: A (Administrative Exempt; straight time)
EEOC: B02 (Professional)
WCC: 9410
JUNE 2021

MINIMUM QUALIFICATIONS:

Mandatory Requirements (conditions of employment)

- Must have and maintain a valid and unrestricted state issued driver's license (from any state).

- Must agree to submit to and successfully pass a state background check, and must be eligible to obtain and maintain a "SECRET" security clearance through the U.S. Department of Homeland Security. *(At a minimum, a favorable suitability determination by the State Security Manager is required prior to appointment into this position.)*

- Travel is required for training and job performance. Must agree to travel by all modes of transportation and stay at destinations for moderate to extended periods of time.

- Must agree to attend/accomplish required training and participate in training exercises as identified in federal grant guidance, by the IOEM Training and Exercise Program, and by IOEM Senior Management; must agree to successfully complete online courses as determined by the same.

- Must have, or be eligible and willing to obtain, a U.S. Passport for international travel to foreign destinations (i.e. Canada).

- Must have the required education and/or months of specialized experience indicated below.

    - A Bachelor's degree (*) or higher an accredited 4-year college or university in the Information Technology (IT) or cybersecurity field; **OR**

    - A Bachelor's degree (*) or higher from an accredited 4-year college or university in any field. Major course work in the Information Technology (IT) field or cybersecurity is preferred; **AND**
    - Three (3) years minimum of relevant professional work experience in the IT or cybersecurity field

      * Required education may be substituted on a year-for-year basis by related professional work experience that includes any combination of the following primary duties and responsibilities: knowledge and skill using systems security principles and concepts of emerging Information Technology (IT) security developments; primary duties directed within the infrastructure protection environment and the selection of appropriate tools; the development or adaptation of applications, systems or networks.

Preferred education/training (**not mandatory**).

- Possession of a professional security management certification such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials.

Knowledge, Skills and Abilities (KSAs)
Applicants must have 36-months of specialized experience performing related duties as specified below.

- Knowledge of Information Security frameworks such as NIST, the CIS Critical Security Controls, Federal Information Security Management Act (FISMA), and Governance, Risk and Compliance (GRC), now referred to as Integrated Risk Management (IRM).

- Knowledge of, and experience with, the federal Critical Infrastructure/Key Resource Program and its goals.

- Working knowledge of emergency/disaster response mechanisms and the ability to interact effectively with a variety of local, state, tribal and federal agencies as well as the citizens of Idaho.

- Knowledge of Risk Management processes.

- Skill in communicating at the organizational level. Oral and written communication skills demonstrating logic, focus, critical thinking, and clarity. Skill in negotiation, compromise, and collaborative problem solving. Skill in appropriate delegation of responsibility and authority. Use of interpersonal skills to create collaborative/cooperative environments.

- Knowledge of the National Incident Management System (NIMS) and Incident Command System (ICS).

- Skill in preparing effective plans and providing knowledgeable comments during the review of planning documents.

- Ability to interact successfully with a wide range of public and private sector organizations and individuals.

- Experience in developing and executing a budget.

CONDITIONS OF EMPLOYMENT:
a. Each person hired will be required to provide verification of eligibility to work in the United States and may be subject to a criminal background check.
b. Refer to the position description for the Mandatory Requirements for this position.
c. The State of Idaho, Military Division is an Equal Opportunity employer. Selection for this position will be made without regard to race, color, religion, national origin, sex (including gender identity, sexual orientation, and pregnancy), genetic information, political affiliation, marital status, and disability or age (which does not interfere with job accomplishment or job eligibility based upon the position description Mandatory Requirements). Appropriate consideration shall be given to veterans in accordance with applicable state and federal laws and regulations.

PERSONNEL MANAGER CERTIFICATION: The title, series, grade, duties and responsibilities are complete and accurate as written and a current or projected vacancy exists as advertised.

Gloria A. Duncan
Supervisory Human Resource Specialist
Military Division – State Personnel Branch

The HRO State Personnel Branch will not forward incomplete application packets for consideration.

SUPPLEMENTAL INFORMATION:

If you are unable to apply online, please contact the HRO office by phone 208-801-4273 or email hrobypass@imd.idaho.gov to discuss alternative options.

Thank you for your interest in employment with the Idaho Military Division.

APPLICATIONS MAY BE FILED ONLINE AT:
https://www.governmentjobs.com/careers/idaho

304 North 8th Street
Boise, ID 83720

idhr@dhr.idaho.gov

Position #21-105-N
IOEM CYBERSECURITY PROGRAM MANAGER AND CRITICAL INFRASTRUCTURE KEY RESOURCES (CIKR) PLANNER
GD

IOEM Cybersecurity Program Manager and Critical Infrastructure Key Resources (CIKR) Planner Supplemental Questionnaire

* 1. **Mandatory Requirement (condition of employment)**: Must have and maintain a valid and unrestricted state issued driver's license (from any state).

Provide written response regarding your willingness and ability to meet this condition of employment (have and maintain). DO NOT provide license info here

* 2. **Mandatory Requirement (condition of employment)**: Must submit to and successfully pass a state background check, and must be eligible to obtain and maintain a "SECRET" security clearance through the U.S. Department of Homeland Security. (*At a minimum, a favorable suitability determination by the State Security Manager is required prior to appointment into this position.)*

Provide written response regarding your eligibility, willingness and ability to meet this condition of employment.

* 3. **Mandatory Requirement (condition of employment)**: Travel is required for training and job performance. Must be willing to travel by all modes of transportation and stay at destinations for moderate to extended periods of time.

Provide written response regarding your eligibility, willingness and ability to meet this condition of employment.

* 4. **Mandatory Requirement (condition of employment)**: Must agree to attend/accomplish required training and participate in training exercises as identified in federal grant guidance, by the IOEM Training and Exercise Program, and by IOEM Senior Management; must agree to successfully complete online courses as determined by the same.

Provide written response regarding your willingness and ability to meet this condition of employment.

* 5. **Mandatory Requirement (condition of employment)**: Must have, or be eligible and willing to obtain, a U.S. Passport for international travel to foreign destinations (i.e. Canada).

Provide written response regarding your eligibility, willingness and ability to meet this condition of employment.

* 6. **Mandatory Requirement (condition of employment)**: Must have the required education and/or months of specialized experience indicated below. . (***Attach supporting documentation*** *to your application; unofficial transcripts are accepted. Describe qualifying work experience(s) including type(s) and duration*)

• A Bachelor's degree (*) or higher an accredited 4-year college or university in the Information Technology (IT) or cybersecurity field; **OR**
• A Bachelor's degree (*) or higher from an accredited 4-year college or university in any field. *Major course work in the Information Technology (IT) field or cybersecurity is preferred*; **AND**
• Three (3) years minimum of relevant professional work experience in the IT or cybersecurity field

* Required education may be substituted on a year-for-year basis by related professional work experience that includes any combination of the following primary duties and responsibilities: knowledge and skill using systems security principles and concepts of emerging Information Technology (IT) security developments; primary duties directed within the infrastructure protection environment and the selection of appropriate tools; the development or adaptation of applications, systems or networks.

Provide written response how you meet this condition of employment (if applicable for experience, describe experience in detail)

7. Preferred education/training (**not mandatory**). *If applicable, provide written response to certification held and* ***attach a copy to your application.***
•Possession of a professional security management certification such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials.

* 8. KSA: **Knowledge of Information Security frameworks such as NIST, the CIS Critical Security Controls, Federal Information Security Management Act (FISMA), and Governance, Risk and Compliance (GRC), now referred to as Integrated Risk Management (IRM).**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement. *Response should be detailed and include specific examples of job duties performed, responsibilities, etc.*

* 9. KSA: **Knowledge of, and experience with, the federal Critical Infrastructure/Key Resource Program and its goals.**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement. *Response should be detailed and include specific examples of job duties performed, responsibilities, etc.*

* 10. KSA: **Working knowledge of emergency/disaster response mechanisms and the ability to interact effectively with a variety of local, state, tribal and federal agencies as well as the citizens of Idaho.**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement. *Response should be detailed and include specific examples of job duties performed, responsibilities, etc.*

* 11. KSA: **Knowledge of Risk Management processes.**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement. *Response should be detailed and include specific examples of job duties performed, responsibilities, etc.*

* 12. KSA: **Skill in communicating at the organizational level. Oral and written communication skills demonstrating logic, focus, critical thinking, and clarity. Skill in negotiation, compromise, and collaborative problem solving. Skill in appropriate delegation of responsibility and authority. Use of interpersonal skills to create collaborative/cooperative environments.**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement. *Response should be detailed and include specific examples of job duties performed, responsibilities, etc.*

* 13. KSA: **Knowledge of the National Incident Management System (NIMS) and Incident Command System (ICS).**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement. *Response should be detailed and include specific examples of job duties performed, responsibilities, etc.*

* 14. KSA: **Skill in preparing effective plans and providing knowledgeable comments during the review of planning documents.**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement.

Response should be detailed and include specific examples of job duties performed, responsibilities, etc.

* 15. KSA: **Ability to interact successfully with a wide range of public and private sector organizations and individuals.**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement. *Response should be detailed and include specific examples of job duties performed, responsibilities, etc.*

* 16. KSA: **Experience in developing and executing a budget.**

Provide detailed written response describing your specialized experience performing related duties to demonstrate that you meet the minimum **36-month** requirement. *Response should be detailed and include specific examples of job duties performed, responsibilities, etc.*

* 17. Unqualified or incomplete applicant packets will not be forwarded.
Do you certify you attached any supporting/required documentation and given detailed written responses with your application packet before submitting?

❑ Yes ❑ No

* 18. Do you certify that all of the information and attached documents to this application are true, correct, complete and made in good faith? (This will constitute your official signature.)

❑ Yes ❑ No

* Required Question