TITLE 21 VACANCY ANNOUNCEMENT

Department of Health and Human Services (HHS)
Food and Drug Administration (FDA)
Center for Devices and Radiological Health (CDRH)
Office of Science and Engineering Laboratories (OST)

Position: Cybersecurity Specialist (Interdisciplinary)

Series: The position of Interdisciplinary position may be filled by candidates from the following occupational series: Computer Engineer (0854), Electronics Engineer (0855), Computer Scientist (1550).

Location(s): Silver Spring, Maryland

Travel Requirements: This position may require up to 25% travel.

Application Period: Monday August 31, 2020 through Wednesday September 30, 2020

Salary: Salary is commensurate with education and experience.

Conditions of Employment: United States Citizenship is required.

Special Notes: This position is being filled under an excepted hiring authority, Title 21, Section 3072 of the 21st Century Cures Act. The candidate selected for this position will serve under a career or career-conditional appointment and be paid under the provisions of the authority. Additional information on 21st Century Cures Act can be found here.

Introduction:
The Food and Drug Administration (FDA or Agency) is the regulatory, scientific, public health and consumer protection agency responsible for ensuring all human and animal drugs, medical devices, cosmetics, foods, food additives, drugs and medicated feeds for food producing animals, tobacco and radiation emitting devices safe, and effective.

The mission of CDRH is to protect and promote the public health by performing essential public health tasks by making sure that medical devices and radiological health products are safe for people in the United States. The Office of Science and Engineering Laboratories (OSEL) supports the CDRH mission of protecting and promoting public health. We undertake the highest quality science to provide our customers with the best methods, tools and expertise to ensure readiness for emerging and innovative medical technologies; develop appropriate evaluation strategies and testing standards; create accessible and understandable public health information; and deliver timely and accurate decisions for products across their life cycle.

Division of All Hazards Response, Science and Strategic Partnerships (DARSS), All Hazard Readiness Response and Cybersecurity (ARC). CDRH's ARC program's mission is to advance national preparedness for Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE), emerging infectious disease, or natural disaster threats by enhancing CDRH's regulatory science capabilities while leveraging an integrated approach to public health emergency operational responsiveness. The ARC Program is uniquely suited to identify and address the legal, regulatory, and scientific challenges that impede the development, and therefore the availability of Medical Countermeasure (MCM) medical devices including diagnostic devices. By expanding the breadth and depth of regulatory science knowledge and expertise that will inform safety and effectiveness evaluation of MCM assets critical for deployment before and during a public health incident, the ARC program facilitates the timely review of all MCM medical devices and diagnostics in CDRH's MCM portfolio.

Furthermore, through the development, implementation, training exercises, and updates to the Center's Emergency Operations plans and procedures, the ARC program is in the best position to deliver on key strategic priorities, spanning the total product lifecycle from pre-event preparedness, to near-real time feedback and through post-event surveillance and monitoring. Ultimately, these efforts are aimed at reducing the cost and / or the time needed to develop a Medical Countermeasure device or diagnostic, enabling a more streamlined path to commercialization and readiness for deployment.

Position Summary:
As the Cybersecurity expert, the selected candidate will work with leading cyber security experts to develop cyber policy, proactively address vulnerabilities, and respond to cyber attacks to protect public health in America. Drive innovative solutions for medical device cybersecurity. Experts will utilize their experience designing, marketing fixing cyber-secure devices. Candidates will use should understand the software industry and the complexity of creating and secure embedded devices to include threat identification and mitigation, vulnerability analysis and risk assessment. Candidates should be comfortable in a fast-paced and flexible environment; able to communicate effectively across all audiences to achieve common goals.

Duties/Responsibilities:
Reporting directly to the Division Director, the incumbent will perform the following duties:

- Analyze and evaluate digital technology and its potential to be introduced into healthcare along with the resulting device cybersecurity impact and shares information with internal and external stakeholders.
- Develop, review, analyze, and improve medical device cybersecurity policy and related regulatory deliverables including how cybersecurity may affect medical device product safety and public health.
- Identify opportunities and risks for modifying CDRH's total product life cycle (from device concept and development to end of life) approach of medical device cybersecurity to promote timely, efficient scientific assessment and review of products.
- Identify emerging technologies that could be used as medical devices and that will be impacted by cybersecurity and makes policy recommendations to mitigate cybersecurity threats and vulnerabilities.

- Identification, analysis and mitigation of cybersecurity threats and vulnerabilities. Able to critically assess vulnerabilities and determine optimal solutions using the most up to date techniques.
- Pre-emptively identifies novel and traditional cybersecurity risks and threats and works with companies on security research to ensure the high-quality cybersecurity protection of medical devices.
- Review and provide feedback on product security analysis for all software and hardware technologies to include radio-frequency identification (RFID), wired and wireless health care technology, encryption, and client authentication, among others.
- Participate with internal team conducting comprehensive investigations and assembles and analyzes data and information on cybersecurity threats and vulnerabilities to medical devices to both internal and external stakeholders.
- Research and provide recommendations on cybersecurity project/program management activities to the Division.
- Proactively identifies technology trends and evolving science that may influence cybersecurity technologies, medical device development, evaluation, and regulatory policy.
- Participate and develop strategies related to cybersecurity with various OST scientific and professional staff, industry, device manufacturers, healthcare providers, patients, staff, and other stakeholders, in the medical device and cybersecurity communities.
- Participate in precedent-setting research to advance patient safety.

Equal Employment Opportunity Policy

The United States Government does not discriminate in employment on the basis of race, color, religion, sex (including pregnancy and gender identity), national origin, political affiliation, sexual orientation, marital status, disability, genetic information, age, membership in an employee organization, retaliation, parental status, military service, or other non-merit factor.

- Equal Employment Opportunity (EEO) for federal employees & job applicants

Reasonable Accommodation Policy

Federal agencies must provide reasonable accommodation to applicants with disabilities where appropriate. Applicants requiring reasonable accommodation for any part of the application process should follow the instructions in the job opportunity announcement. For any part of the remaining hiring process, applicants should contact the hiring agency directly. Determinations on requests for reasonable accommodation will be made on a case-by-case basis.

A reasonable accommodation is any change to a job, the work environment, or the way things are usually done that enables an individual with a disability to apply for a job, perform job duties or receive equal access to job benefits.

Under the Rehabilitation Act of 1973, federal agencies must provide reasonable accommodations when:

- An applicant with a disability needs an accommodation to have an equal opportunity to apply for a job.
- An employee with a disability needs an accommodation to perform the essential job duties or to gain access to the workplace.
- An employee with a disability needs an accommodation to receive equal access to benefits, such as details, training, and office-sponsored events.

You can request a reasonable accommodation at any time during the application or hiring process or while on the job. Requests are considered on a case-by-case basis.

Learn more about disability employment and reasonable accommodations or how to contact an agency.

Professional Experience/Key Requirements:
To qualify for this position, successful candidates will be accomplished and dynamic Cybersecurity professionals. The candidate should have significant experience and expertise in

- Ability to understand a broad range of cybersecurity and the ability to translate information/findings.
- Excellent communication skills.
- Ability to work collaboratively with a diverse cadre of customers and stakeholders.
- Ability to work effectively within teams.
- Ability to prioritize.

Basic Qualifications:
Candidates must possess the required individual occupational requirements to qualify for the appropriate series applicable to the position. Please use the following link to determine the series for which you qualify: https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/#url=List-by-Occupational-Series

Desirable Education:
Applicants with a Ph.D., or an equivalent advanced degree in science, or engineering fields are highly desired.

Conditions of Employment:

- One-year probationary period may be required.
- Background and/or Security investigation required.
- U.S. citizenship is required.
- All applicants born male, on (or after) 12/31/1959, must be registered with the Selective Service System OR have an approved exemption. Visit www.SSS.gov for more info.
- This position is subject to strict prohibited financial interest regulations which could restrict the type of financial interest (stock holdings) for the employee, the spouse, and minor children of the employee. For additional information on the prohibited financial interests, please visit the FDA Ethics and Integrity Office website at https://www.fda.gov/about-fda/jobs-and-training-fda/ethics.

How to Apply:
Prior to applying, please see the following instructions:

- Documents to submit: electronic resume or curriculum vitae, cover letter containing a brief summary of scientific accomplishments, and copy of transcripts
- Compile all applicant documents into **one combined document (i.e. Adobe PDF)**
- Include Job Reference code ***"OSEL-20-LKI-03"*** in the email subject line.
- Email comprehensive applicant package/document OSELRecruitment@fda.hhs.gov by **Wednesday September 30, 2020**.

The Department of Health and Human Services is an equal opportunity employer with a smoke free environment.

FDA is an equal opportunity employer.