1. NAME OF NOMINEE:

Deborah Coleman

2. NOMINEE'S EMPLOYING ORGANIZATION:

US Department of Education

3. NOMINEE'S POSITION AND/OR TITLE:

4. NOMINEE'S PHONE NUMBER:

5. NOMINEE'S E-MAIL ADDRESS:

Qualification Statement (What has the nominee done to warrant this nomination?

Explain how the nominee exemplifies innovation in an awareness and training program and the impact of the program.

6. I nominate (NOMINEE'S NAME AND TITLE) of (NOMINEE'S ORGANIZATION) for the FISSEA 2021 Cybersecurity Awareness and Training Innovator Award.

I nominate Deborah Coleman, Cybersecurity Awareness and Training program manager of the US Department of Education for the FISSEA 2021 Cybersecurity Awareness and Training Innovator Award. Since 2009 Ms. Coleman has worked diligently to enhance and mature the Department's cybersecurity training program. Under her direction, the program has moved beyond just compliance with Federal Information Security Modernization Act (FISMA) of 2014 requirements to a full fledged cybersecurity workforce development program. Current program components include: program governance, cybersecurity & privacy awareness training, organization-wide communications, specialized role-based training (RBT), phishing assessments, and cyber workforce development.

7. Explain how the public sector benefitted from the activities of the nominee. *

In FY2020 Ms. Coleman led the deployment of the Department's Report Phishing button to all ED Outlook email clients; this button allows users to directly report suspicious emails to the Department Security Operations Center (EDSOC) with a single click. When the button is used to report an email delivered as part of an authorized phishing exercise, the user receives immediate feedback in the form of a "Thank you" message. Through these innovations department seen a 50% improvement in reporting rates and a similar decrease in susceptibility. In FY2021, she led the deployment of an email warning banner to warn users about the origination of the email (e.g., outside of the Department) in addition to Department standards of target trainings for repeat risk users through authorized fiscal year phishing campaigns. Ms. Coleman implemented and maintains the Department's cybersecurity workforce development program. She actively participates with interagency workforce development working groups and contributed to the Cyber Career Pathways Tool developed by the Interagency Federal Cyber Career Pathways Working Group. Employees and contractors in roles with significant security responsibilities (SSR) are required to complete cybersecurity role-based training (RBT) annually. Ms. Coleman strives to ensure a wide range of current RBT courses, e-books and videos are made available to these individuals through the Department's learning management system. Instructor-led courses and workshop materials to focus attention on increasing role specific knowledge, skills and abilities. Under her direction in October 2020, the Department conducted its first virtual Cybersecurity Symposium. This symposium was conducted each Thursday throughout the month of October and it provided current information and training to over 500 Department employees and contractors. Ms. Coleman selected and branded the web-based platform used to deliver the symposium, developed the event agenda, and engaged a wide range of informative speakers from within the Department as well as the public and private sectors to support the event. Throughout the event a variety of communications were used to encourage participation. Event attendance was tracked and surveys used to obtain feedback

and cyber training credits. Ms. Coleman and her team launched a refreshed annual cybersecurity & privacy awareness training course which was updated using insights gained from training surveys, phishing data and stakeholder outreach. The course included a new test out feature. Users which demonstrated competency in course knowledge areas by successfully passing the test out feature completed the training in an average of fifteen minutes. This represents an average time savings of thirty minutes per user. The deployment of the ED Report Phishing button, the Department's SOC gained needed visibility to malicious emails which made it through the perimeter into user mailboxes. This visibility allows the Department to stop threats faster. Prior to the deployment of the ED Report Phishing button, the average reporting rate in FY2019 was 15.21%. After the launch of the button, the average reporting rate increased to 30.2% at the end of FY2020. From a "live fire" perspective the Department's SOC has seen a sizable increase in phishing reported via the new reporting capabilities.

8. Describe the impact of the nominee's achievements and accomplishments within and/or beyond the nominee's organization. *

Throughout the pandemic situation, Ms. Coleman developed and delivered a series of awareness articles designed to increase awareness of emerging fraud schemes and scams targeting employees and their families. These timely articles communicated how bad actors were using the public's interest in COVID-19 to obtain personally identifiable information (PII) and money through various schemes; other articles focused attention on attacks against our Nation's largely remote workforce. Each article included tips and information on how to avoid getting scammed and these tips enabled the employee to take action to protect themselves, their families and the Department. In FY2020, Ms. Coleman implemented new processes to identify and maintain a baseline of employees and contractors with significant security responsibilities, including privileged users. Identifying this user base has enabled the Department to gain visibility to and take action to reduce risks originating from privileged users such as failed phishing exercises. Phishing exercise data and reports provide senior leadership with necessary insights to support focused capability development efforts to alleviate the issue of users which repeatedly clicked on suspicious email messages. Through data dissemination and increased messaging of phishing susceptibility risks and a need to increase phishing reporting from the top down across the enterprise and sub agencies. The department saw a trend in the right direction for how users interacted with phishing threats. The information is briefed to the Secretary, Deputy Secretary, Assistance Secretaries and all leadership throughout the Department. Phishing is now a standing agenda item at the senior management meetings and briefings with the Secretary and Deputy Secretary. Department leadership uses the feedback from the phishing and training exercises to reinforce the importance of safe user behavior and actions when working online. With leadership discussing the importance of phishing and cybersecurity, the Department truly has cybersecurity as part of its culture.

9. If any of the activities of the nominee were part of a group effort, indicate the amount and type of direct participation by the nominee as compared to other participants. Describe how the nominee distinguished himself/herself from other members of the group. *

Ms. Coleman led the program, resources, and technical oversight that assisted with the efforts described.

10. Additional information about the nominee that FISSEA should consider. *

Ms. Coleman maintained and enhanced the department cybersecurity training program while the administration change too place and optimal funding levels not met.

11. Person making this nomination: *

ED Chief Information Security Officer, Steven Hernandez

12. Daytime Phone Number and E-Mail Address of Person making the nomination: *