The Office of the National Coordinator for Health Information Technology

ISAO Federal Opportunity Announcement (FOA)

Applicants Webinar

Rose-Marie Nsahlai, Office of the Chief Privacy Officer (OCPO), Lead IT Security Specialist
Libbie Buchele, Office of the Chief Privacy Officer (OCPO), Program Manager
Yolonda Thompson-Teagle, Office of Procurement and Grants (OPG), Senior Grants Specialist

Welcome and Introductions

Welcome & Introductions

- Rose-Marie Nsahlai, Office of the Chief Privacy Officer (OCPO), Lead IT Security Specialist
- Libbie Buchele, Office of the Chief Privacy Officer (OCPO), Program Manager
- Yolonda Thompson-Teagle, Office of Procurement and Grants (OPG), Senior Grants Specialist

Format: we will provide an overview of the FOA and eligibility criteria. Questions will be documented but we may not respond to all questions on the call.

About this information session

- This teleconference is being recorded. If you object please disconnect now
- Teleconference slides and recording will be available after the teleconference at https://www.healthit.gov/newsroom/onc-funding-cyber-threat-information-sharing-health-care-and-public-health-hph-sector.
- Please submit questions to the chat box during the presentation. Any question not addressed in the FOA will be collected and evaluated, and answered in the form of FAQs
- After the call, questions should be submitted in writing to onc_ocpogrants@hhs.gov. We will post the responses to all questions to grants.gov. The FAQs can also be viewed at https://www.healthit.gov/newsroom/onc-funding-cyber-threat-information-sharing-health-care-and-public-health-hph-sector.

Background and Overview

Background

- Section 3001(b) of the HITECH Act established ONC, in part, to support the development of a nationwide health information technology infrastructure.
- One of ONC's guiding principles for nationwide interoperability in the health IT infrastructure is to "protect privacy and security in all aspects of interoperability." (Principle #3, *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*).
- To support this guiding principle, ONC committed to "coordinate with the Office of the Assistant Secretary for Preparedness and Response (ASPR) on priority issues related to cybersecurity for critical public health infrastructure" (Commitment #C3.3).

Background-Continued

- As recent news reports show, security breaches and ransomware attacks in the Healthcare and Public Health sector are on the rise. Criminal cyber attacks against health care organizations are up 125 percent compared to five years ago, replacing employee negligence and lost or stolen laptops as the top cause of health care data breaches. The average consolidated total cost of a data breach was $3.8 million, a 23 percent increase from 2013 to 2015.
- To better prevent attacks on health information technology, organizations need better visibility into what to expect and how to respond. Therefore, for the past three years, ONC has worked in partnership with the Assistant Secretary for Preparedness and Response (ASPR), the Office of the Assistant Secretary for Administration (ASA),the Office of the Chief Information Officer's (OCIO) Office of Information Security (OIS), and the Office of Security and Strategic Information's (OSSI) Cyber Threat Intelligence Program (CTIP) to develop the means to facilitate cyber threat information sharing across the Healthcare and Public Health sector.

Key Drivers

- **Cybersecurity Information Sharing Act (CISA)**
  - Outlines new requirements for cyber threat information sharing.
  - Section 405(c) of the Act establishes Health Care Industry Cybersecurity Task Force. Section 405 (c) (1) (D) and 405 (c) (1) (E) outline the task force's duties regarding recommendations for cybersecurity threat information dissemination, including establishing a plan for federal Government and Health Care and Public Health (HPH) sector stakeholders to share actionable cyber threat indicators and defensive measures.

Key Drivers-Continued

- Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, defined HHS's information sharing role with respect to cybersecurity threats. EO 13636 calls on HHS to participate with other Sector-Specific Agencies and the Department of Homeland Security to "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."

Key Drivers-Continued

On February 13 2015, the President signed Executive Order (EO) 13691, Promoting Private Sector Cybersecurity Information Sharing.

EO 13691 encourages the development of information sharing and analysis organizations (ISAOs) to serve as focal points for cybersecurity collaboration within the private sector and between the private sector and government.

- This broadens existing terminology related to information sharing and analysis centers (ISACs), by identifying ISACs as one type of organization among other types of ISAOs.

Purpose of the Grant

- This Funding Opportunity Announcement (FOA) announces a cooperative agreement funding opportunity for an existing ISAO or ISAC for the Health Care and Public Health (HPH) sector.
- The purpose of this cooperative agreement is to build the capacity of information sharing and analysis organizations (ISAO) to share cyber threat information (CTI) bi-directionally between HHS and the HPH sector about cyber threats and to provide outreach and education to the HPH sector. The goal is to improve cyber security awareness within the sector and to equip sector stakeholders to take action in response to CTI shared by the ISAO.

Grant Program Objectives

This Funding Opportunity Announcement (FOA) is intended to fill a gap by providing resources to *broaden* access to enable CTI sharing and dissemination of that information across the HPH sector. **There will be one recipient.** It is expected that the recipient will be able to:

1. Build internal resources to serve as a single ISAO
2. Expand its current membership base;
3. Focus more of its business and resources on CTI sharing;
4. Create a lower entry cost for smaller HPH sector organizations who wish to join an ISAO; and
5. Eventually provide some level of free CTI sharing services to the entire HPH sector.

Additional information

Who should apply?

- It is anticipated that the chosen recipient will be an entity that is already providing outreach and technical assistance to participating organizations on cyber threats.

Partnership:

- As there will be a single award, the government encourages separate organizations to develop the mechanism to collaborate on a single application if doing so would strengthen the overall capacity of the “eventual” ISAO.

Purpose of the Informational Session

- Discuss the background, purpose, scope, terms and conditions and other provisions in the FOA
- Explain the eligibility and application requirements
- Describe the application review process
- Provide an opportunity for interested parties to ask questions

Overarching Goal

The Funding Opportunity Announcements released by ONC for an existing ISAO or Information Sharing and Analysis Center (ISAC) to:

- Provide cybersecurity information and education on cyber threats affecting the Healthcare and Public Health sector
- Expand outreach and education activities to assure that information about cybersecurity awareness is available to the entire Healthcare and Public Health sector
- Equip stakeholders to take action in response to cyber threat information
- Facilitate information sharing widely within the Healthcare and Public Health Sector, regardless of the size of the organization

Structure and Approach

The project will be broken out into three distinct Phases.

- Phase 1: “Preparation and Infrastructure Building” will be completed within the first two years of the project period.
- Phase 2: “Serving as an ISAO” will be completed in years two through five.
- Phase 3: “Sustainability of the ISAO” will be completed by the end of year five and is expected to continue after the end of the grant award.

Phase 1: Preparation and Infrastructure Building

Year 1 Targets Include:

1. Develop and expand infrastructure for coaching small & medium size health care organizations regarding steps they can take when they become aware of cyber threats

2. Actively seek to enrich recipient's current cyber threat indicators by providing additional context to define meaning of the indicators, make corrections, or any suggested improvements.

3. Federal agencies currently provide several resources for ISAOs to leverage at no cost, and are in the process of formulating additional resources. Specifically, the recipient shall build upon and connect with the resources identified in Table A-Resources, as well as others that would facilitate the process of CTI sharing in the HPH sector:

Phase 1: Preparation and Infrastructure Building

continued

Year 2 Targets Include:

1. Continue to establish and expand collaborations with key HPH sector stakeholder groups to ensure adequate dissemination, education, and awareness of cyber threats, security and privacy vulnerabilities, and incidents .

2. Begin to provide cybersecurity awareness and education on immediate cyber threats affecting the HPH sector to new health care and public health organizations. Information shall include translating CTI into plain language and providing mitigation strategies for a specific threat that can be understood by different types of HPH sector stakeholders

Phase 2: Serving as an ISAO

Year 3 Targets Include:

1. Provide cybersecurity awareness and education on immediate cyber threats affecting the HPH sector to new organizations in the sector. One of the key tasks shall include translating CTI into plain language and providing mitigation strategies for a specific threat that can be understood by different types of HPH sector stakeholders

2. Develop cybersecurity education and training materials and tools for the HPH sector for different types of audiences and provide an efficient way to disseminate this information to the entire sector (Outreach), and support localized training to reach HPH sub-sector organizations across the U.S.

Key Details of ONC's FOA

Type of Award	Cooperative Agreement
Available Funding	$250,000
Number of Awards	1
Award Ceiling	$250,000
Application Due Date	8/19/2016
Anticipated Award Date	9/16/2016
Performance Period	5 years
Anticipated Start Date	9/26/2016

Key Dates

Milestone	Date
FOA Released	*July 20, 2016*
Informational Session	**August 11, 2016**
Notice of Intent Due	*August 1,2016*
Applications Due	*August 19, 2016*
Anticipated Award Date	*September 16, 2016*
Anticipated Project Start Date	*September 26, 2016*
Cooperative Agreement Period of Performance	*September 26, 2016 to September 25, 2021*

Applicant's Eligibility

- Local, Public nonprofit institution/organizations, Private nonprofit institution/organization, Private and for profit organizations that are already providing outreach and technical assistance to participating organizations on cybersecurity threats.
- Organization that currently provides CTI sharing services to some parts of the HPH sector and seeks to expand the reach of those services.
- Organization that provides CTI sharing services to a sector other than HPH, and seeks to expand their services to the HPH sector.

Applicant's Eligibility-Continued

- **Note:** Two or more organizations can work together to apply under a single application for this FOA.
- Partnership in CTI sharing is always beneficial.
- Have a Dun & Bradstreet (D&B) Universal Numbering System (DUNS) number.
- Register in the System for Award Management (SAM) at www.sam.gov; allow a minimum of 5 days to complete the registration. If you are already registered in SAM and have not renewed your registration in the last 12 months, you must renew your registration.

Application Package- Full Application

- Project Abstract
- Project Narrative
- Form SF-424, Application for Federal Assistance 21
- Form SF-424A, Budget Information for Non-Construction Programs
- Form SF-424B, Assurances for Non-Construction Programs
- Form SF-LLL, Disclosure of Lobbying Activities
- Budget Narrative
- Project Plan
- Letters of Commitment
- Proof of Non-Profit Status (if, applicable)
- Indirect Cost Agreement(s) – including recipient, sub-recipient, and contractors agreements (if applicable)

Application Contents (Full Application)-Continued

Project Abstract: 500 word maximum to include the following:

I. Project Title

II. Applicant Name

III. Physical Address

IV. Contact Name

V. Contact Phone Numbers (Voice, Fax)

VI. E-Mail Address

VII. Web Site Address, if applicable

Application Contents (Full Application)-Continued

Project Narrative

- The project narrative should address the elements articulated in the Program Description/Purpose and Structure and Approach sections of the FOA.
- The project narrative should also align with the Performance Goals/Program Milestones and Merit Review Evaluation criteria presented in this FOA (e.g., organizational experience, past performance).
- Must be double-spaced, formatted to 8 ½" x 11" (letter-size) pages, 1" margins on all sides, and a font size of not less than 11 point.
- The maximum length allowed for the Project Narrative is ***20* pages**. A Project Narrative that exceeds the *20* page limit may not be considered for further review.
- Resumes of Key Personnel, if requested, are not counted as part of the Project Narrative and are not included in the *20* page limit.

Application Contents (Full Application)-Continued

Project Approach:

- The current infrastructure and resources that exist in their organization and how they will expand their infrastructure to achieve the proposed objectives and deliverables of the project;
- A description of how the applicant will use ONC funds in the first few years of the cooperative agreement to build additional subject matter expertise and capacity for education and outreach to the HPH sector;
- A description of how the applicant will use this additional capacity to meet the objective to expand its reach and perform broader outreach and education and increase its membership base in phase two of the cooperative agreement
- Identification of strategies to implement educational cybersecurity tools and disseminate those tools to the HPH sector;

Application Contents (Full Application)-Continued

Budget Narrative/Justification

- Appendix D provides a template to complete the budget narrative populated with sample information. **The budget narrative must not exceed 1 page in length**.
- When more than 33% of a Project's total budget falls under a contractual expense, a detailed Budget Narrative/Justification must be provided for each sub-contractor or sub-recipient.
- The Budget Narrative must be double-spaced, formatted to 8 ½" x 11" (letter-size) pages, 1" margins on all sides, and a font size of not less than 11 point.
- Costs may not be incurred until the beginning date of the award
- The duration of this award is for a maximum of 5 years. The budget and justification must reflect the costs for the initial 12- month budget period.
- Applicants must submit a proposal which covers the full 5-year project period. Although initial funding awarded through this FOA will cover only the first 12-month budget period of the 60 month project period, applicants must still submit an estimated budget for each budget period (years 1, 2, 3, 4, and 5).

Application Contents (Full Application)-Continued

Project Plan

The Project Plan must identify important objectives and deliverables associated with the Project, including:

1. The current infrastructure and resources that exist in their organization and how they will expand their infrastructure to achieve the proposed objectives and deliverables of the project;
2. A discussion of the provisional findings identified by the provisional ASPR Report discussed in the background section, including an assessment of the current state of the HPH infrastructure's technical readiness and information sharing activities and a discussion to illustrate how they are applied to advance interoperable health IT systems;
3. Identification of strategies to implement educational cybersecurity tools and disseminate those tools to the HPH sector; and
4. A sustainability plan that would allow for continuous sharing of CTI post grant period.

Application Contents (Full Application)
Project Plan- Continued

Project Plans must include baseline measurements for each of the established objectives. Types of metrics could include but are not limited to:

- Timeliness of disseminating CTI to HPH stakeholders
- Educational/training sessions conducted
- Review of CTI and cyber indicators; providing guidance to HPH stakeholders
- Establish a baseline of how much of the HPH sector the organization currently reaches; expand outreach by X % per year
- Progress towards use of and leveraging of resources of other federal agencies and prominent cyber authoritative sources of information

Evaluation Criteria

Evaluation Criteria

- Organizational Capacity (30 points)
- Technical Expertise (25 points)
- Technical Approach (25 points)
- Management Approach (10 points)
- Budget Allocation (10 points)

Criteria I: Organizational Capacity (30 Points)

- Does the applicant organization clearly identify in their Project Plan capacity for carrying out the proposed project?
- Does the organization have established working relationships with key sector organizations and government agencies that can be leveraged to expand outreach across the HPH sector?
- Does the applicant organization have existing and proven CTI sharing capabilities that could be expanded under this cooperative agreement?
- Does the applicant clearly describe a plan for sustainability post grant period?

Criteria II- Technical Expertise (25 Points)

- Does the applicant organization possess knowledge of the structure and organization of the Health care and Public Health sector, key sector cybersecurity risks, relevant cybersecurity policies and industry standards, CTI sharing processes, and sources of CTI?
- Can the applicant describe where cyber threat sharing is occurring effectively now, and where it is not, and why the difference?
- Does the organization have proven experience in these matters?

Criteria II- Technical Expertise (25 Points)- Continued

- Does the applicant demonstrate an understanding of the findings from the gap analysis described in Section A Program Description/Purpose and propose a means of addressing these findings?
- Does the applicant demonstrate an understanding of CISA and applicable Executive Orders?
- Has the applicant provided an analysis of other emerging policies that may affect information sharing, including the CISA and the automated information sharing requirement?

Criteria III-Technical Approach (25 points)

- Is the applicant's technical approach to implementing this project likely to lead to successful completion of the project objectives?

Criteria IV: Management Approach (10 points)

- Does the applicant organization propose a management approach that is expected to lead to the efficient and appropriate use of resources to accomplish the project objectives while ensuring high quality of work?
- Are activities in each year clearly defined?

Criteria V-Budget Allocation (10 points)

- Is the budget justified with respect to the reasonableness of resources requested?
- Are budget line items clearly delineated and consistent with the Project Plan objectives?

ISAO Grant

ONC Program Office

ONC Office of the Chief Privacy Officer (OCPO)

Provides analysis and education in response to privacy and security needs generated as a result of the evolution of the digital health information ecosystem. Advises the National Coordinator, other HHS agencies, other branches of government, and states.

OCPO's Primary Functions

Coordinate efforts to ensure that key privacy and security protections are in place to achieve public trust in Health IT adoption, health information exchange, and meaningful use.

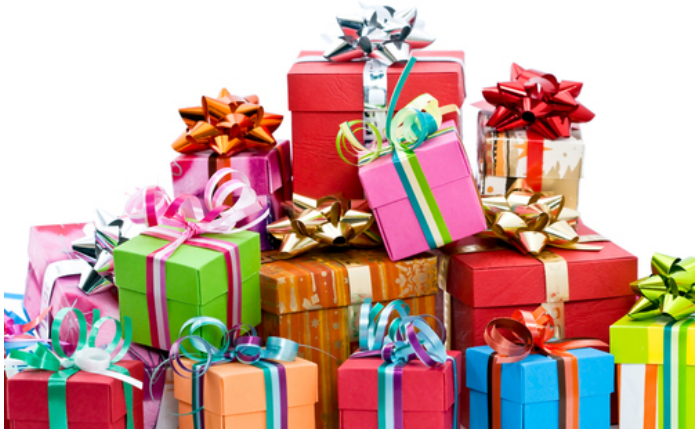
OCPO's Responsibilities

Develop and coordinate privacy, security, and data stewardship policy across the federal government, state and regional agencies, and foreign countries by providing subject matter expertise and technical support

Additional information

- Thank you for attending!
- We will remain online for 5 minutes – please submit any remaining questions via the web conferencing system
- Any questions not already addressed will be added to the FAQ
- If you have additional questions, please submit them in writing to ONC OCPO Grants onc_ocpogrants@hhs.gov
- For the FAQ and additional information on this FOA, go to
- https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/opportunity-sharing-information-cyber-attacks/
- To see the FOA on grants.gov or to apply, go to http://www.grants.gov/view-opportunity.html?oppId=286509
- For assistance with submitting applications in Grants.gov, please contact the Grants.gov Helpdesk at support@grants.gov or call at 1-800-518-4726

Wrapping It Up…Thank You!



- Thank you to everyone for participating. ONC would like to thank ASPR and OCIO's Office of Information Security (OIS), and the Office of Security and Strategic Information's (OSSI) Cyber Threat Intelligence Program (CTIP) for their partnership and commitment to this effort