

Advisory Committee Meetings dated April 15, 2016.

Dated: March 14, 2022.

Samuel Roth,

Attorney-Advisor, National Endowment for the Humanities.

[FR Doc. 2022-05652 Filed 3-16-22; 8:45 am]

BILLING CODE 7536-01-P

NATIONAL SCIENCE FOUNDATION

Request for Information on Federal Priorities for Information Integrity Research and Development

AGENCY: Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO) and National Science Foundation (NSF).

ACTION: Request for information.

SUMMARY: The NITRD NCO and the NSF, as part of an interagency working group on information integrity, request input from interested parties on a range of questions pertaining to Federal priorities for research and development efforts to address misinformation and disinformation. The purpose of this RFI is to understand ways in which the Federal Government might enable research and development activities to advance the trustworthiness of information, mitigate the effects of information manipulation, and foster an environment of trust and resilience in which individuals can be discerning consumers of information.

DATES: Interested persons or organizations are invited to submit comments on or before 11:59 p.m. (EST) on May 15, 2022.

ADDRESSES: Comments submitted in response to this notice may be sent by the following methods:

- *Email:* IIRD-RFI@nitrd.gov. Email submissions should be machine-readable and not be copy-protected. Submissions should include "RFI Response: Information Integrity R&D" in the subject line of the message.

- *Mail:* Attn: Tomas Vagoun, NCO, 2415 Eisenhower Avenue, Alexandria, VA 22314, USA.

Instructions: Response to this RFI is voluntary. Each individual or organization is requested to submit only one response. Submissions must not exceed 10 pages in 12 point or larger font, with a page number provided on each page. Responses should include the name of the person(s) or organization(s) filing the comment. Responses to this RFI may be posted online at <https://www.nitrd.gov>. Therefore, no business proprietary

information, copyrighted information, or other personally identifiable information should be submitted in response to this RFI.

In accordance with FAR 15.202(3), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFI.

FOR FURTHER INFORMATION CONTACT:

Tomas Vagoun at IIRD-RFI@nitrd.gov or 202-459-9685, or by post mailing to NCO, 2415 Eisenhower Avenue, Alexandria, VA 22314, USA.

Individuals who use a telecommunications device for the deaf (TDD) may call the Federal Information Relay Service (FIRS) at 1-800-877-8339 between 8 a.m. and 8 p.m., ET, Monday through Friday.

SUPPLEMENTARY INFORMATION:

Background: Accurate and reliable information is central to our Nation's democratic, economic, geopolitical, and security interests, guiding decisions that impact the well-being of society. Information that is, knowingly or unknowingly, manipulated and disseminated for political, ideological, or commercial gain can have destabilizing consequences for democratic processes, the economy, individual health and well-being, the environment, local and national crisis response efforts, human rights and protections, and national security. New technological advances have enabled manipulated information [1] to reach vast audiences around the world at an unprecedented speed. Thus, preserving the *integrity* of information—ensuring our society is protected against information manipulation—is of national importance.

As announced by the White House [2], Federal Government agencies have formed the Information Integrity Research and Development Interagency Working Group (IIRD IWG) to develop a strategic plan concerning government-wide research and development. The purposes of IIRD IWG are to better understand the full information ecosystem, to design strategies for preserving information integrity and mitigating the effects of information manipulation, to support information awareness and education, and to foster a multi-disciplinary and collaborative research environment in which to reach deeper understanding, while upholding these information integrity goals.

Information Requested: Protecting the integrity of the information ecosystem requires an understanding of: Actors and consumers of information

(including individuals, organizations, and nation states) and their different capabilities, actions, plans, and intentions; strategies and technologies for creating, disseminating, and sharing manipulated information; solutions for detecting and mitigating information manipulation across a wide range of information media, forms, and communication modalities; social, psychological, and physiological responses to experiencing information manipulation; ways to increase public awareness of information manipulation; the societal benefits of accurate information and vibrant discussion; and protections of the First Amendment.

The IIRD IWG seeks public input on Federal priorities for information integrity research and development (R&D). Responders are asked to answer one or more of the following questions:

1. *Understanding the information ecosystem:* There are many components, interactions, incentives, social, psychological, physiological, and technological aspects, and other considerations that can be used to effectively characterize the information ecosystem. What are the key research challenges in providing a common foundation for understanding information manipulation within this complex information ecosystem?

2. *Preserving information integrity and mitigating the effects of information manipulation:* Strategies for protecting information integrity must integrate the best technical, social, behavioral, cultural, and equitable approaches. These strategies should accomplish a range of objectives including to detect information manipulation, discern the influence mechanisms and the targets of the influence activities, mitigate information manipulation, assess how individuals and organizations are likely to respond, and build resiliency against information manipulation. What are the key gaps in knowledge or capabilities that research should focus on, in order to advance these objectives? What are the gaps in knowledge regarding the differential impact of information manipulation and mitigations on different demographic groups?

3. *Information awareness and education:* A key element of information integrity is to foster resilient and empowered individuals and institutions that can identify and abate manipulated information and create and utilize trustworthy information. What issues should research focus on to understand the barriers to greater public awareness of information manipulation? What challenges should research focus on to support the development of effective educational pathways?

4. *Barriers for research:* Information integrity is a complex and multidisciplinary problem with many technical, social, and policy challenges that requires the sharing of expertise, data, and practices across the full spectrum of stakeholders, both domestically and internationally. What are the key barriers for conducting information integrity R&D? How could those barriers be remedied?

5. *Transition to practice:* How can the Federal government foster the rapid transfer of information integrity R&D insights and results into practice, for the timely benefit of stakeholders and society?

6. *Relevant activities:* What other research and development strategies, plans, or activities, domestic or in other countries, including in multi-lateral organizations and within the private sector, should inform the U.S. Federal information integrity R&D strategic plan?

7. *Support for technological advancement:* How can the Federal information integrity R&D strategic plan support the White House Office of Science and Technology Policy's mission:

- Ensuring the United States leads the world in technologies that are critical to our economic prosperity and national security; and
- maintaining the core values behind America's scientific leadership, including openness, transparency, honesty, equity, fair competition, objectivity, and democratic values.

References

- [1] "Manipulated information" refers to information content that is inaccurate, misleading, or deceptive within the context of its intended use and that has the effect of causing harm to individuals, communities, or institutions. "Information manipulation" refers to activities that aim to influence specific or multiple audiences through disinformation, misinformation, malinformation, propaganda, manipulated media, and other tactics and techniques that intentionally create or disseminate inaccurate, misleading, or unreliable information.
- [2] FACT SHEET: The Biden-Harris Administration is Taking Action to Restore and Strengthen American Democracy (December 8, 2021), The White House, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/08/fact-sheet-the-biden-harris-administration-is-taking-action-to-restore-and-strengthen-american-democracy/>.

Submitted by the National Science Foundation in support of the Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO) on March 14, 2022.

(Authority: 42 U.S.C. 1861.)

Suzanne H. Plimpton,
Reports Clearance Officer, National Science Foundation.

[FR Doc. 2022-05683 Filed 3-16-22; 8:45 am]

BILLING CODE 7555-01-P

POSTAL SERVICE

Privacy Act of 1974; System of Records

AGENCY: Postal Service™.

ACTION: Notice of modified systems of records.

SUMMARY: The United States Postal Service® (Postal Service) is proposing to revise a Customer Privacy Act System of Records (SOR). These modifications are being made to store, send, and host emails for Informed Delivery on a cloud-based platform.

DATES: These revisions will become effective without further notice on April 18, 2022, unless in response to comments received on or before that date result in a contrary determination.

ADDRESSES: Comments may be submitted via email to the Privacy and Records Management Office, United States Postal Service Headquarters (privacy@usps.gov). To facilitate public inspection, arrangements to view copies of any written comments received will be made upon request.

FOR FURTHER INFORMATION CONTACT: Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202-268-3069 or privacy@usps.gov.

SUPPLEMENTARY INFORMATION: This notice is in accordance with the Privacy Act requirement that agencies publish their systems of records in the **Federal Register** when there is a revision, change, or addition, or when the agency establishes a new system of records. The Postal Service has determined that Customer Privacy Act System of Records, USPS 820.300 Informed Delivery, should be revised to support the migration of emails to a cloud-based platform.

I. Background

The Postal Service has determined that Customer Privacy Act Systems of Records (SOR), USPS 820.300 Informed Delivery, should be revised to store, send, and host emails for Informed Delivery on a cloud-based platform.

II. Rationale for Changes to USPS Privacy Act Systems of Records

The Postal Service constantly seeks to improve efficiency and customer

satisfaction. To that end, the Postal Service seeks to implement a new hosting service for Informed Delivery Daily Digest emails through the cloud, replacing the current on-premises solutions.

III. Description of the Modified System of Records

To implement the change to a cloud-based platform, this System of Records will be modified to include several new categories of records, numbered 11 through 21, to identify data elements associated with Daily Digest emails which will be collected and stored as part of this migration. In addition, a new purpose has been added to identify this new process. Finally, a retention period for the records generated in association with these activities has been added.

Pursuant to 5 U.S.C. 552a (e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the proposed revisions has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect this amended system of records to have any adverse effect on individual privacy rights. The notice for USPS SOR 820.300, Informed Delivery is provided below in its entirety, as follows:

SYSTEM NAME AND NUMBER

USPS 820.300, Informed Delivery.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

USPS Headquarters; Contractor Sites; Cloud-based Contractor Sites; Wilkes-Barre Solutions Center; and Eagan, MN.

SYSTEM MANAGER(S):

Vice President, Innovative Business Technology, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1010.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 403, and 404.

PURPOSE(S) OF THE SYSTEM:

1. To support the Informed Delivery® notification service which provides customers with electronic notification of physical mail that is intended for delivery at the customer's address.

2. To provide daily email communication to consumers with images of the letter-size mailpieces that they can expect to be delivered to their mailbox each day.

3. To provide an enhanced customer experience and convenience for mail delivery services by linking physical mail to electronic content.