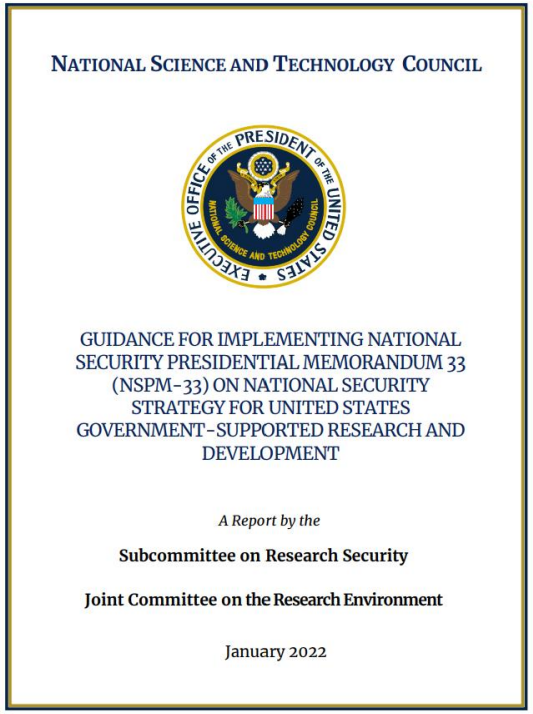
Digital Persistent Identifiers (DPIs)

Northeastern University
Research Enterprise Services

Why are we talking about DPIs?

NSPM-33

- "*Provide guidance to Federal departments and agencies regarding their implementation of National Security Presidential Memorandum 33 on National Security Strategy for US Government-Supported Research and Development*".
- Guidance requires a certification from research institutions awarded more than $50 million per year total in Federal research funding confirming they have implemented a research security program meeting the requirements.
- Guidance requires within 1 year of the date of the memorandum, "*funding agencies shall establish policies regarding requirements for individual researchers supported by or working on any Federal research grant to be registered with a service that provides a digital persistent identifier for that individual*".
- NSPM-33 gives DPIs implementation guidance stating that DPIs should be integrated wherever possible.



NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

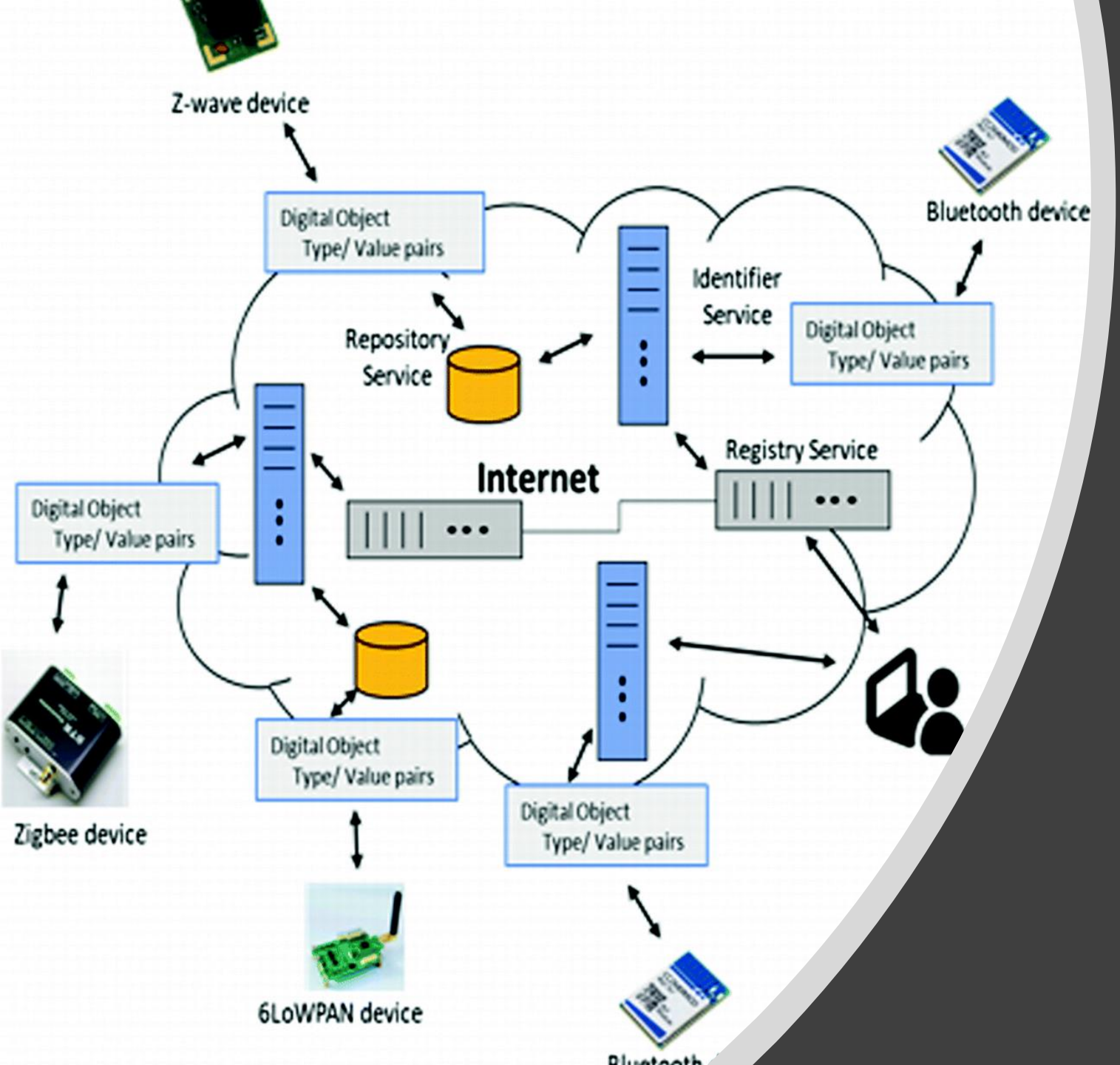
GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

A Report by the

Subcommittee on Research Security

Joint Committee on the Research Environment

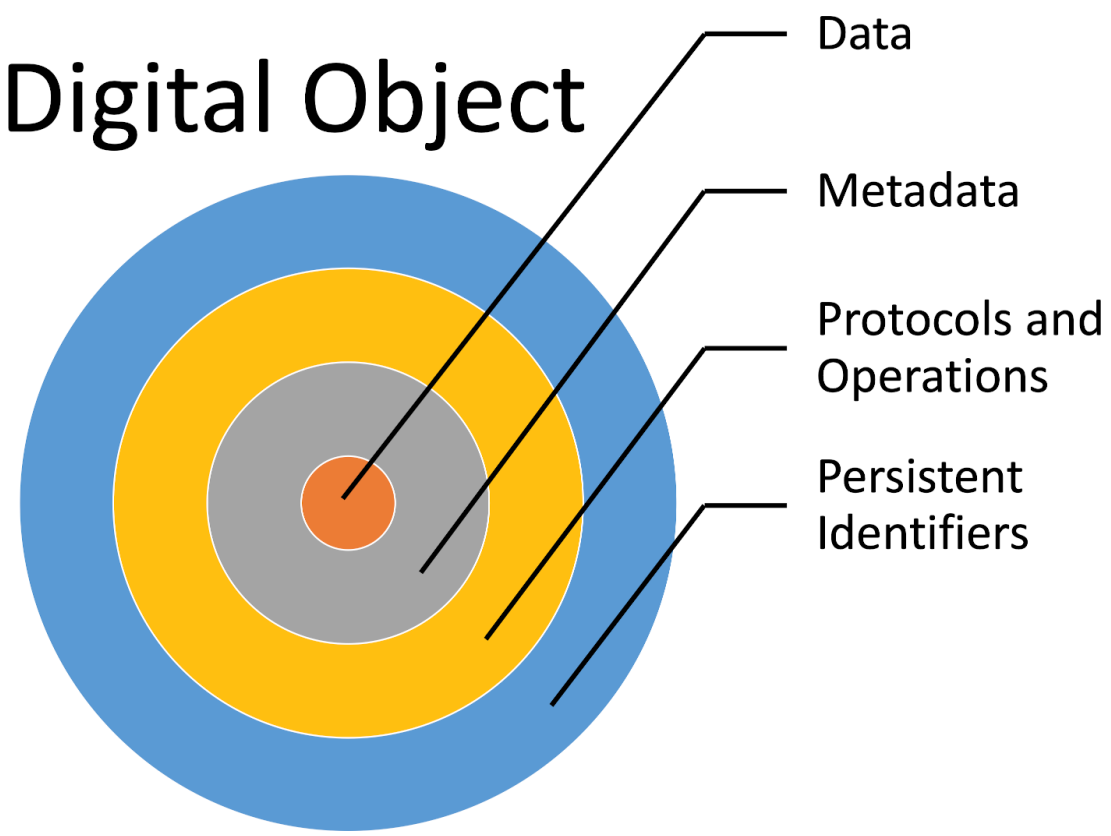
January 2022



Understanding the Digital Object Architecture

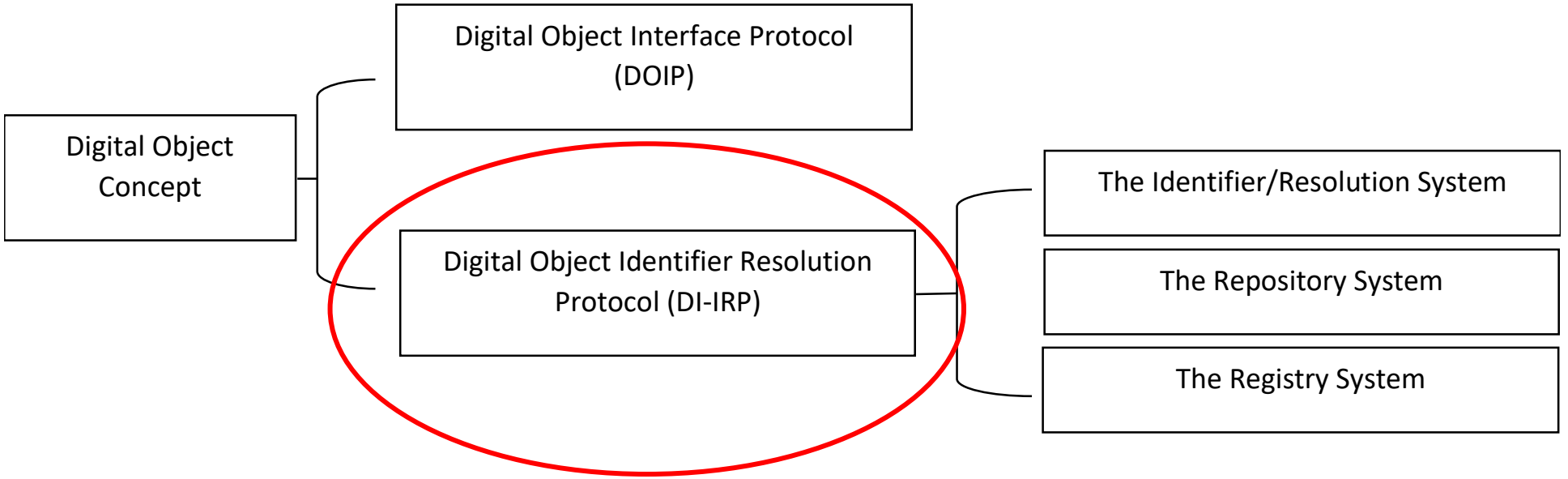
Digital Object Architecture

- General architecture for distributed information storage, location and a retrieval system running over the internet
  - Data: collection of images, string of words, set of facts
  - Metadata: provides meaningful information about the data
  - Protocols: instructions on how to retrieve the data
  - ← Identifiers: how the data is identified
- DOA supports FAIR Data Principles
  - Identifier must be globally unique: unable to be reused/reassigned to a different individual
  - Identifier must be persistent: registry services prevent links from becoming invalid



Digital Object Concept

- A digital object is a sequence of bits (or a set) incorporating a work or portion of a work or other information in which a party has rights or interests (i.e. text file)
- Digital objects are vulnerable to damage - become physically damaged through degradation over time (i.e. USBs), unavailable through loss of access (i.e. Cloud service closes), or software/hardware obsolescence (i.e. Floppy drives).



Three Core Components

1. The Identifier System

- Allotment of unique identifiers to information in digital form structured as digital objects

2. The Repository System

- The repository system manages digital objects including the provision of access to such objects based on the use of identifiers, and with integrated security.

3. The Registry System

- The registry system stores metadata about digital objects rather than the digital information itself.
- Typically stores metadata of digital objects that are managed by one or more repository systems.

ORCID

Connecting Research
and Researchers

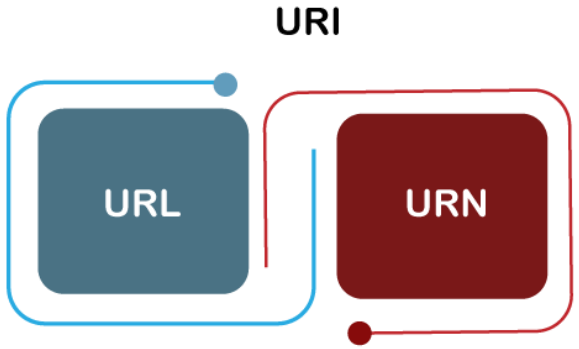
The Identifier System

What is a Digital Object Identifier (DOI)?

- DOI is a unique, persistent identifying number for information published online that appears on a document or in a bibliographic citation
- Becoming the international standard for making research data citable
- DOI consists of two components: prefix and suffix. Components are separated by a slash
- If you encounter a DOI on a website, it is preceded by three letters: "doi"
- The DOI itself begins with a 10; the registration agency (i.e. DataCite) is responsible for the following four or more digits of the prefix. They belong to the organization (i.e. DataCite) which registered the dataset.
- The suffix is assigned by the institution (i.e. Northeastern) that is responsible for the content and registered the dataset.

What is a Digital Persistent Identifier (DPI)?

- A DPI is a long-lasting digital reference to an object, contributor, or organization
- A code which remains constant to the digital object it is assigned to for identification purposes, regardless of changes to its location on the internet



ARK Alliance

PURL

ORCID
Connecting Research and Researchers

Benefits of Digital Persistent Identifiers (DPIs)

- Help to establish the authenticity of a resource

←Provides access to a resource even if its location changes (link stops working)

←Bypasses problems caused by the impermanent nature of URLs

←Allows interoperability between collections

←DPIs are widely established/widely deployed

←Will help mitigate issues researchers currently face when distinguishing their research activities from those of other with similar names

←DPIs will allow researchers to uniquely connect their identity to research objects such as datasets, equipment, articles, media stories, citations, experiments, and patents.

←Save researchers time from re-entering the same personal data repeatedly

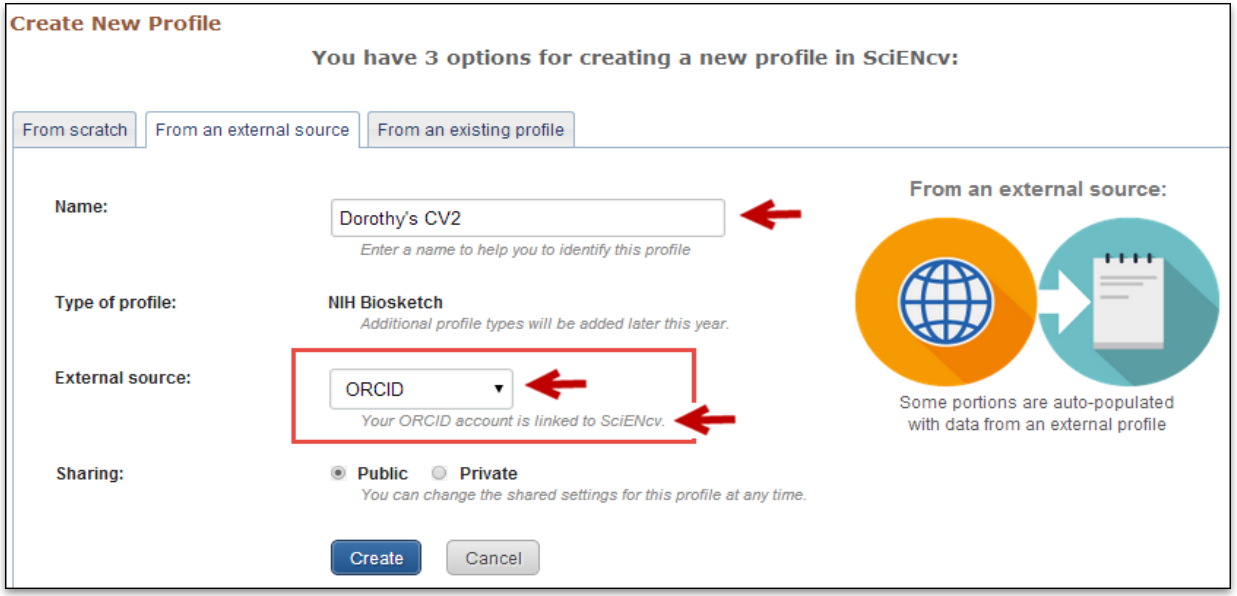
DOI vs. DPI

DOI – *link to academic products* (Digital Object Identifier)	**DPI – *link to PI's academic profile* (Digital Persistent Identifier)**
▪ "Digital identifier of an object" - can be assigned to any digital object	▪ Connects researcher to their product. A profile to link PI to their products.
▪ DataCite: Provides digital object identifiers (DOIs) for research data, and scholarly and technical publications.	▪ ORCID iD: Provides *researchers* with a DPI (ORCID iD), that they own and control, which distinguishes individuals. ▪ Professional information can be connected and shared with other systems, ensuring recognition for all research contributions.

Why use ORCID?

- Meets the criteria as a DPI as listed in the NSPM-33 Guidance
- Provides unique IDs that distinguish researchers from one another regardless of their name
- Allows researchers to create a single record that represents their CV
- Provides a workflow to discourage multiple records for a single person and the ability to consolidate duplicate IDs
- Reduces administrative burden on researchers by enabling the transfer of authorized data between systems
- Assigns IDs to researchers at no charge
- Allows the researcher to control access to the information in their ORCID profile; they can determine what information is displayed publicly, what is shared with trusted partners, and who those trusted partners are
- Is easily integrated with NIH & NSF's digital CV system "SciENcv"

SciENcv System



	iD	NIH Biosketch
1.	Bibliography	Personal Statement
2.	Employment	Positions and Honors
3.	Education	Education/Training
4.	Works	Citations & Contribution to Science
5.	Funding	Additional Information: Research Support and Scholastic Performance

1. Researchers can import data from their ORCID profiles into SciENcv

2. SciENcv maps the ORCID profile fields into the relevant biosketch format

ORCID

Connecting Research and Researchers

The Repository System

ORCID Repository System

- ORICD can be used in repository systems to clearly link authors (and their name variants) with their research work, improving search and retrieval to support networking and collaboration
- ORCID API allows repository systems to exchange data with the ORCID Registry to populate local author profiles
- ORCID records can also be updated with publication information each time a repository deposit is made

ORCID API – Public vs. Member

- Public API – allows organizations that are not ORCID members to connect their systems
- Member API – facilitates registration and information exchange with ORCID records

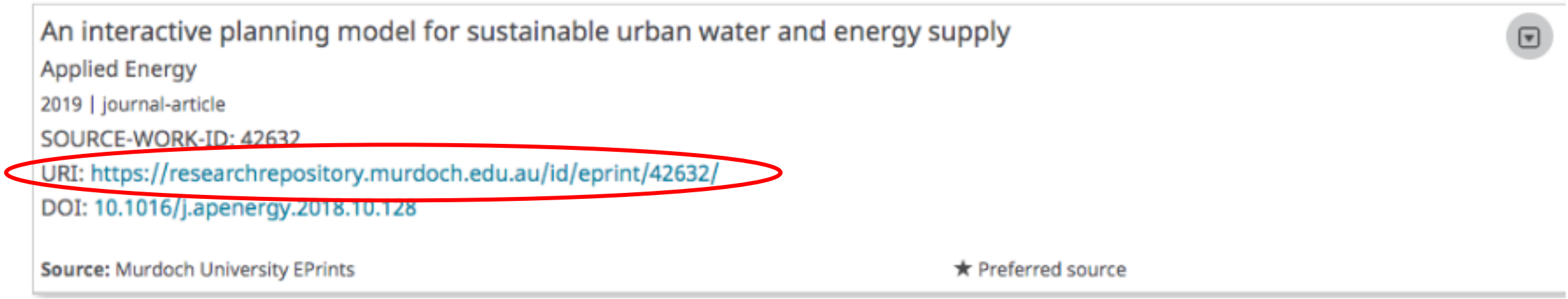
ORCID Public API	ORCID Member API
Sign into system with ORICD	Sign into system with ORICD
Get a user's verified ORICD iD	Get a user's verified ORICD iD
Retrieve public data from a user's ORCID record	Retrieve public data from a user's ORCID record
Search public ORCID registry data	Search public ORCID registry data
	Access trusted data
	Write data to ORICD records
	Synchronize ORCID with institution's system

How does the Repository work?

- The repository collects the researchers authenticated ORCID iD and requests permission to interact with their record, storing that permission
  - This allows the administrators to request authenticated ORCID iDs and ORCID record update permissions from authors and co-authors, in cases where iDs are missing/have not been authenticated in the metadata received
- Once the researcher has connected their ORCID iD to the institutions system, their iD will be displayed on their profile (formatted as a hyperlinked URI) within the institutions system so that they know they have successfully connected and asserted their identity.
- With the researcher's permission:
  - Publications on the researcher's ORCID record can be added to the institution's repository
  - Researcher's ORCID record can be updated with the publications that are available within the repository

Example

- This is an example of a work added by Murdock University via their EPrints integration repository system



ORCID

Connecting Research and Researchers

The Registry System

ORCID Registry System

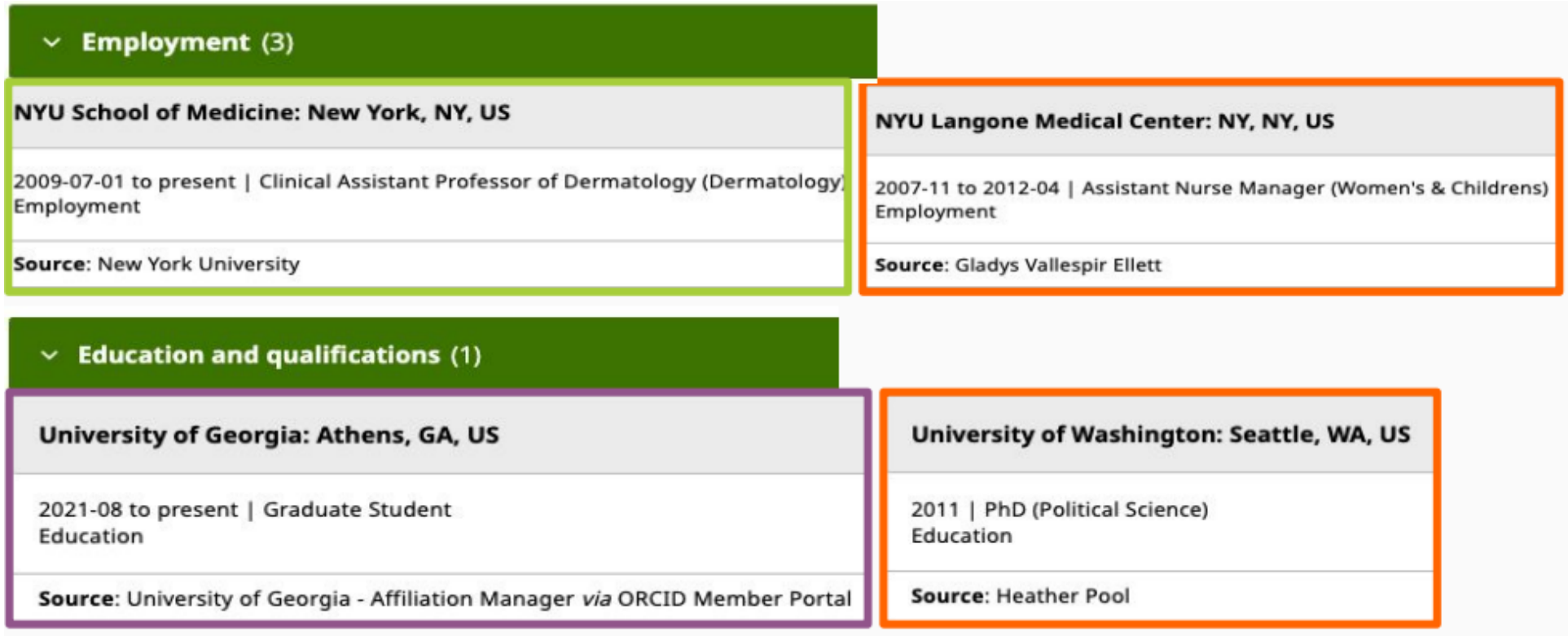
- ORICD provides a registry of unique identifiers for researchers and scholars that is open, non-proprietary, transparent, and mobile.
- ORCID invites all researchers to participate without entry fees or maintenance costs.
- Researchers can sign in and maintain their record, including adding, updating, and deleting items and setting their privacy levels
- Researchers can grant ORCID member integrations permissions to read trusted data and/or update their record as part of a member workflow. Previously granted permissions can be removed at any time.

Add a trusted individual to ORCID account

- ORCID makes it easy to give a Research Administrator access and permissions to update and manage an ORCID profile
- Researchers should **NOT** give their Research Administrator their ORCID account credentials (username and/or password)
- Instead, researchers should visit the following link to learn how to add a trusted individual to your account: Trusted Parties
- Trusted individuals, also known as Account Delegates, are other ORCID iD holders to whom the researcher has granted permission to update their ORCID record.
- Access can be granted or revoked at any time.

Increase trustworthiness of ORCID records

- Member universities can increase the trustworthiness of ORCID records by writing validating data to researcher's records (with their permission)
- University is a "Trusted Organization"



Recap: DPIs

Digital Persistent Identifier Recap

WHAT

- A DPI is a long-lasting digital reference to an object, contributor, or organization
- A code which remains constant to the digital object it is assigned to for identification purposes, regardless of changes to its location on the internet

WHERE

- **ORCID**: 1. The Identifier, 2. The Repository and 3. The Registry

WHY

- Researchers can connect their identity to research objects such as datasets, equipment, articles, citations, experiments, and patents.
- Give the researcher control access to the information in their ORCID profile; publicly displayed information; what information is shared with trusted partners, and who those trusted partners are; ability to give/revoke trusted access

Three Core Components

1. The Identifier System → • ORICID iD – unique identifier per researcher

2. The Repository System → • ORCID API – allows repository systems link authors (and all their name variants) to improve search and retrieval to support networking and collaboration.

3. The Registry System → • ORCID Registry – populates local author profiles; registry of unique identifiers for researchers and scholars that is open, non-proprietary, transparent and mobile; free of cost

Questions

Contact Us

NU-RES Research Compliance

ResearchCompliance@northeastern.edu