The Exploring the Durability of PURLs and Their Alternatives Working Group of the Depository Library Council recommends the Council endorse these Principles for PIDs and PID systems, and further recommends they be transmitted to the Director of GPO with a recommendation that they be adopted. 05/02/2023

Recommended Principles for Persistent Identifiers and Persistent Identifier Systems for the Government Publishing Office

The Depository Library Council convened the Exploring the Durability of PURLs and Their Alternatives Working Group to examine the benefits and drawbacks of the persistent URL system currently used by the Government Publishing Office (GPO), and to explore the current landscape for persistent identifiers (PIDs) more broadly. The Working Group identified a need for principles to guide the determination of the best available solution for persistent access to Federal Government information in the current digital landscape. The Working Group subsequently created the following recommended principles for PIDs and PID systems for GPO. The Working Group incorporated GPO's vision of *America Informed* through free permanent public access to the U.S. Government's information into the development of these principles, and sought to consider the current state of Federal information technology infrastructure and cybersecurity.

PERSISTENT IDENTIFIER PRINCIPLES

PIDs must be unique and provide direct long-term access to a specific digital document or object that is openly accessible.

Each PID is associated with a unique and unduplicated URL that provides direct access. There is a one-to-one correlation between the PID and the digital object it identifies. PIDs should only be assigned to resources that will be preserved for the long term, which is to be understood over several hardware and software generations. GPO should employ PIDs only for digital objects that are openly accessible and can be viewed and downloaded without passing through a paywall.

PIDs must be unchanging and never reused.

The PID for the content must remain the same and should persist over time as long as the resource is publicly accessible. PIDs must never be reused for a different document or object.

PIDs must enable access to a digital resource under the control of a trusted entity or an established partner.

A core component of permanence and reliable performance is control of the digital content. GPO should employ PIDs only for digital objects that are under its control or under the control of an official partner, with a signed agreement requiring the transfer of content if the official partner is unable to maintain it in its current system.

PIDs must enable access to the specific object described in the metadata for the resource.

PIDs must resolve to the version of the resource indicated in the descriptive metadata that is validated or approved by GPO or an official partner. Resources must be disambiguated within the system so they are distinct and distinguishable from other resources. PIDs must be usable for different types of digital content and scalable for increasing amounts of content.

PERSISTENT IDENTIFIER SYSTEM PRINCIPLES

PIDs must be part of a system that is stable, secure, and interoperable with other systems.

The PID system(s) must provide reliable and stable access, with appropriate redundancy against outages and security issues. The system must connect and exchange information with tools, systems, and technologies used by GPO and others. PIDs must be able to be migrated with future system updates.

The PID system must resolve the identifier to the kernel metadata.

A review of the kernel metadata will enable validation that the PID resolves to the intended digital object.

PIDs should work regardless of the users' access starting point and the access system or delivery service used.

URLs that resolve through the PID system(s) should work reliably from any point of origin, allowing local systems to pass traffic through additional controls (such as a proxy server) as needed.

PIDs must have publicly accessible metadata.

PIDs must have metadata that is separate from the object metadata. PID metadata should be publicly accessible, retrievable, and interoperable with global registries.