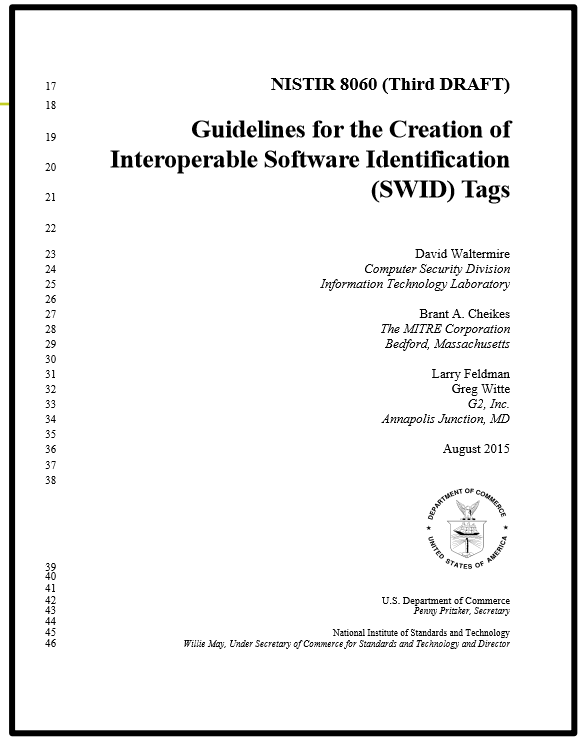
Guidance and Usage Scenarios for Implementers and Users of Software Identification Tags

Brant A. Cheikes

bcheikes@mitre.org

9 September 2015



NISTIR 8060 (Third DRAFT)

Guidelines for the Creation of Interoperable Software Identification (SWID) Tags

David Waltermire
Computer Security Division
Information Technology Laboratory

Brant A. Cheikes
The MITRE Corporation
Bedford, Massachusetts

Larry Feldman
Greg Witte
G2, Inc.
Annapolis Junction, MD

August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

MITRE

Today's Objectives

- **What's a software identification (SWID) tag?**
- **Cybersecurity value of SWID tags**
- **NIST's commitment**
- **Overview of NIST Interagency Report 8060 (3rd Public Draft)**
  - Purpose
  - Audience
  - Document Organization
  - Guidelines and Usage scenarios
- **Open Issues and Next Steps**
- **Concluding Remarks**

What's a SWID Tag? Problem Statement

- **Software is critical infrastructure**
- **Software Asset Management (SAM) is a critical business function**
  - control and protection of software and related assets
  - control and protection of information needed to control and protect software assets
- **Critical challenges:**
  - Installation media are hard to verify
  - Once installed, software applications are hard to *discover*, *identify*, and *characterize*
    - Patches and upgrades too!
  - Relationships among software applications, components, libraries, files, and other system resources are unclear

What's a SWID Tag? The Elevator Speech

An XML Document – Conforms to ISO/IEC 19770-2:2015

```
<SoftwareIdentity
  name="ACME Roadrunner Detector 2013 Coyote Edition"
  tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0" version="4.1.5">
  <Entity name="The ACME Corporation"
          regid="acme.com" role="tagCreator softwareCreator"/>
  <Entity name="Coyote Services, Inc."
          regid="mycoyote.com" role="distributor"/>
  <Link rel="license" href="www.gnu.org/licenses/gpl.txt/">
  <Meta activationStatus="trial" product="Roadrunner Detector"
        colloquialVersion="2013" edition="coyote"/>
  <Payload>
    <Directory root="%programdata%" location="rrdetector">
      <File name="rrdetector.exe" size="532712"
       SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569cd50fd5ddb4d1bbafd2b6a"/>
      <File name="sensors.dll" size="13295"
       SHA256:hash="54e6c3f569cd50fd5ddb4d1bbafd2b6ac4128c2dc663ae7a6b6bc67875940573"/>
    </Directory>
  </Payload>
</SoftwareIdentity>
```

What's a SWID Tag? The Elevator Speech

Minimal Requirements for a Basic Tag

```
<SoftwareIdentity
   name="ACME Roadrunner Detector 2013 Coyote Edition"
   tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0">
   <Entity name="The ACME Corporation"
           regid="acme.com" role="tagCreator"/>
</SoftwareIdentity>
```

Most Elements and Attributes are Optional

What's a SWID Tag? The Elevator Speech

Created by Authoritative Sources (Ideally) or Third Parties

```
<SoftwareIdentity
  name="ACME Roadrunner Detector 2013 Coyote Edition"
  tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0" version="4.1.5">
  <Entity name="The ACME Corporation"
          regid="acme.com" role="tagCreator softwareCreator"/>
  <Entity name="Coyote Services, Inc."
          regid="mycoyote.com" role="distributor"/>
  <Link rel="license" href="www.gnu.org/licenses/gpl.txt/">
  <Meta activationStatus="trial" product="Roadrunner Detector"
        colloquialVersion="2013" edition="coyote"/>
  <Payload>
    <Directory root="%programdata%" location="rrdetector">
      <File name="rrdetector.exe" size="532712"
       SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569cd50fd5ddb4d1bbafd2b6a"/>
      <File name="sensors.dll" size="13295"
       SHA256:hash="54e6c3f569cd50fd5ddb4d1bbafd2b6ac4128c2dc663ae7a6b6bc67875940573"/>
    </Directory>
  </Payload>
</SoftwareIdentity>
```


MITRE

What's a SWID Tag? The Elevator Speech

Uniquely Identifies the Product

```
<SoftwareIdentity
  name="ACME Roadrunner Detector 2013 Coyote Edition"
  tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0" version="4.1.5">
  <Entity name="The ACME Corporation"
          regid="acme.com" role="tagCreator softwareCreator"/>
  <Entity name="Coyote Services, Inc."
          regid="mycoyote.com" role="distributor"/>
  <Link rel="license" href="www.gnu.org/licenses/gpl.txt/">
  <Meta activationStatus="trial" product="Roadrunner Detector"
        colloquialVersion="2013" edition="coyote"/>
  <Payload>
    <Directory root="%programdata%" location="rrdetector">
      <File name="rrdetector.exe" size="532712"
       SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569cd50fd5ddb4d1bbafd2b6a"/>
      <File name="sensors.dll" size="13295"
       SHA256:hash="54e6c3f569cd50fd5ddb4d1bbafd2b6ac4128c2dc663ae7a6b6bc67875940573"/>
    </Directory>
  </Payload>
</SoftwareIdentity>
```


MITRE

What's a SWID Tag? The Elevator Speech

Associates the Product with Tag Creator, etc.

```
<SoftwareIdentity
  name="ACME Roadrunner Detector 2013 Coyote Edition"
  tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0" version="4.1.5">
  <Entity name="The ACME Corporation"
          regid="acme.com" role="tagCreator softwareCreator"/>
  <Entity name="Coyote Services, Inc."
          regid="mycoyote.com" role="distributor"/>
  <Link rel="license" href="www.gnu.org/licenses/gpl.txt/">
  <Meta activationStatus="trial" product="Roadrunner Detector"
        colloquialVersion="2013" edition="coyote"/>
  <Payload>
    <Directory root="%programdata%" location="rrdetector">
      <File name="rrdetector.exe" size="532712"
       SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569cd50fd5ddb4d1bbafd2b6a"/>
      <File name="sensors.dll" size="13295"
       SHA256:hash="54e6c3f569cd50fd5ddb4d1bbafd2b6ac4128c2dc663ae7a6b6bc67875940573"/>
    </Directory>
  </Payload>
</SoftwareIdentity>
```


MITRE

What's a SWID Tag? The Elevator Speech

Associates the Product with Related Information Sources

```
<SoftwareIdentity
  name="ACME Roadrunner Detector 2013 Coyote Edition"
  tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0" version="4.1.5">
  <Entity name="The ACME Corporation"
          regid="acme.com" role="tagCreator softwareCreator"/>
  <Entity name="Coyote Services, Inc."
          regid="mycoyote.com" role="distributor"/>
  <Link rel="license" href="www.gnu.org/licenses/gpl.txt/">
  <Meta activationStatus="trial" product="Roadrunner Detector"
        colloquialVersion="2013" edition="coyote"/>
  <Payload>
    <Directory root="%programdata%" location="rrdetector">
      <File name="rrdetector.exe" size="532712"
       SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569cd50fd5ddb4d1bbafd2b6a"/>
      <File name="sensors.dll" size="13295"
       SHA256:hash="54e6c3f569cd50fd5ddb4d1bbafd2b6ac4128c2dc663ae7a6b6bc67875940573"/>
    </Directory>
  </Payload>
</SoftwareIdentity>
```


MITRE

What's a SWID Tag? The Elevator Speech

Provides Descriptive Metadata

```
<SoftwareIdentity
  name="ACME Roadrunner Detector 2013 Coyote Edition"
  tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0" version="4.1.5">
  <Entity name="The ACME Corporation"
          regid="acme.com" role="tagCreator softwareCreator"/>
  <Entity name="Coyote Services, Inc."
          regid="mycoyote.com" role="distributor"/>
  <Link rel="license" href="www.gnu.org/licenses/gpl.txt/">
  <Meta activationStatus="trial" product="Roadrunner Detector"
        colloquialVersion="2013" edition="coyote"/>
  <Payload>
    <Directory root="%programdata%" location="rrdetector">
      <File name="rrdetector.exe" size="532712"
       SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569cd50fd5ddb4d1bbafd2b6a"/>
      <File name="sensors.dll" size="13295"
       SHA256:hash="54e6c3f569cd50fd5ddb4d1bbafd2b6ac4128c2dc663ae7a6b6bc67875940573"/>
    </Directory>
  </Payload>
</SoftwareIdentity>
```


MITRE

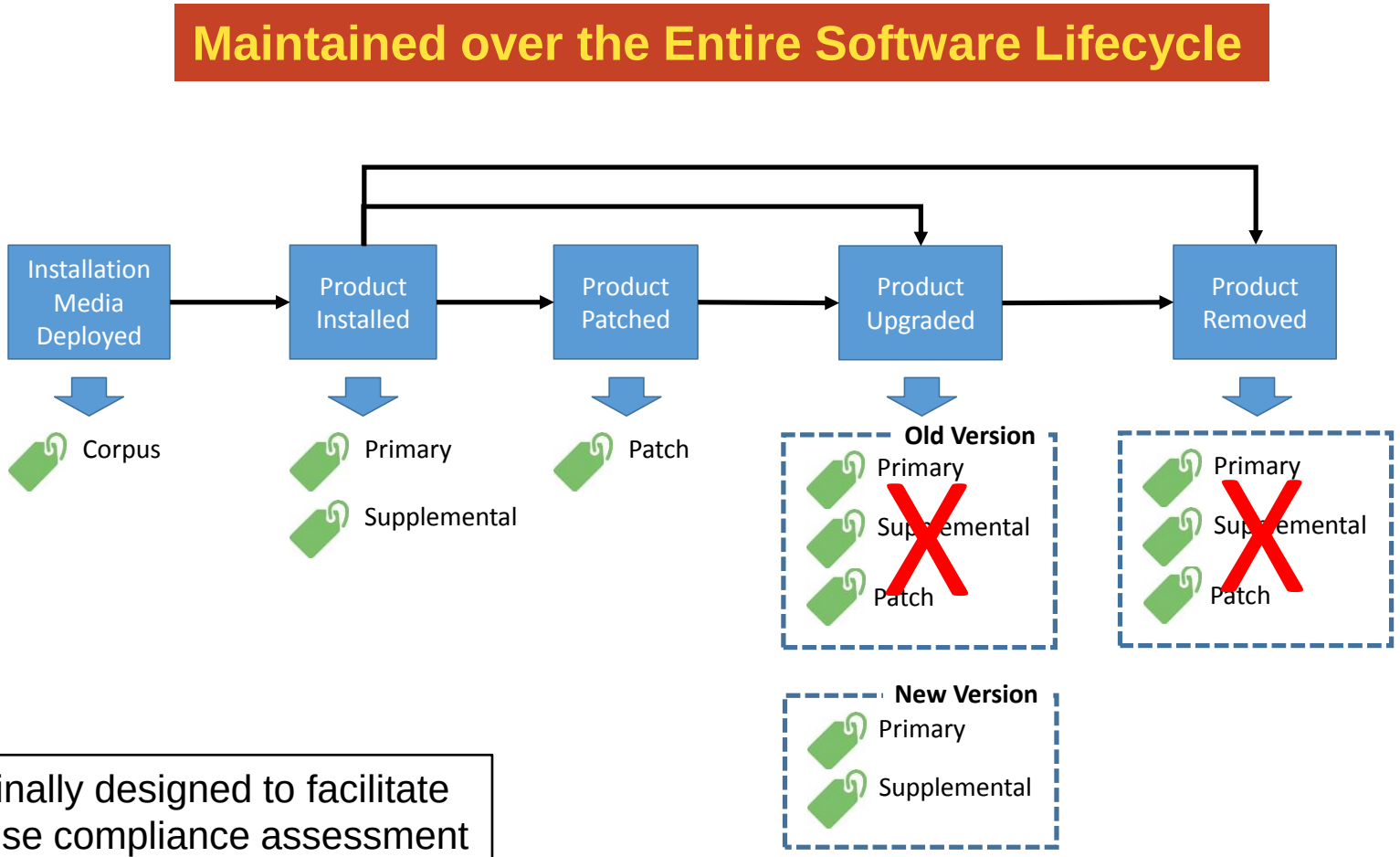
What's a SWID Tag? The Elevator Speech

Characterizes the Product in Detail

```
<SoftwareIdentity
  name="ACME Roadrunner Detector 2013 Coyote Edition"
  tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0" version="4.1.5">
  <Entity name="The ACME Corporation"
          regid="acme.com" role="tagCreator softwareCreator"/>
  <Entity name="Coyote Services, Inc."
          regid="mycoyote.com" role="distributor"/>
  <Link rel="license" href="www.gnu.org/licenses/gpl.txt/">
  <Meta activationStatus="trial" product="Roadrunner Detector"
        colloquialVersion="2013" edition="coyote"/>
  <Payload>
    <Directory root="%programdata%" location="rrdetector">
      <File name="rrdetector.exe" size="532712"
       SHA256:hash="a314fc2dc663ae7a6b6bc6787594057396e6b3f569cd50fd5ddb4d1bbafd2b6a"/>
      <File name="sensors.dll" size="13295"
       SHA256:hash="54e6c3f569cd50fd5ddb4d1bbafd2b6ac4128c2dc663ae7a6b6bc67875940573"/>
    </Directory>
  </Payload>
</SoftwareIdentity>
```


MITRE

What's a SWID Tag? The Elevator Speech



Originally designed to facilitate license compliance assessment

MITRE

Potential Cybersecurity Value of SWID Tags

- **Simplifies software discovery**
  - Helps you know what's out there running on the network
- **Enhances interoperability**
  - Cybersecurity products and services can exchange information about software in a standard format
- **Supports automated continuous monitoring services**
  - Changes to endpoint software inventories may be rapidly detected
  - Tags contain data useful for correlating with security advisories, vulnerability reports, and threat intelligence

NIST's Commitment to SWID Tags

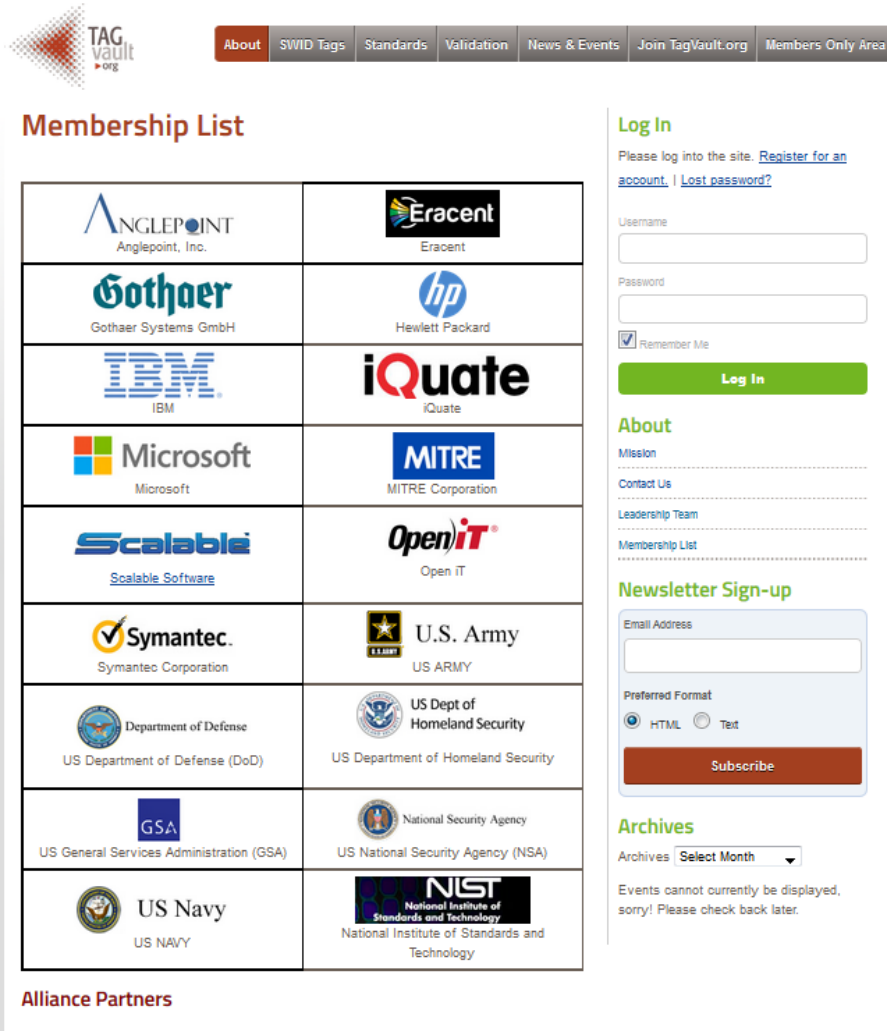
- **Supports SWID tags as eventual replacement to Common Platform Enumeration (CPE) names**

- **Seeks to promote industry adoption by:**
  - Promulgating implementation guidance and best practices
  - Publicly releasing reference implementations and support tools
  - Integrating support for SWID tags into the National Vulnerability Database (NVD)
  - Working with industry and agency partners to maintain and refine the standard over time
  - Promoting interoperability of SWID tags with other standards (e.g., SCAP)

- **NIST Interagency Report 8060 is first public step**
  - *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags—Third Public Draft*
  - Comment period ends 21 September!

TagVault.org

- **Neutral not-for-profit certification authority for software tagging**
- **Industry evangelist for the adoption, use and evolution of interoperable, internationally-accepted standards software identification standards and processes**



NIST IR 8060: Purpose

- **Provide a high-level description of SWID tags in order to increase familiarity with the standard**

- **Provide tag implementation guidelines that supplement the ISO/IEC SWID tag specification**
  - Some guidelines in SWID specification are *strengthened*
  - New guidelines added to increase clarity and reduce ambiguity
  - Guidelines intended solely to extend and not to conflict with any guidelines provided by the SWID specification
  - Guidelines may support future Government acquisition requirements

- **Present a set of operational usage scenarios illustrating how SWID tags conforming to these guidelines can be used to achieve a variety of cybersecurity goals**

NIST IR 8060: Audience

- **Software Providers**
  - Individuals and organizations that develop, license, and/or distribute commercial, open source, and custom software products
- **Providers of Inventory-Based Products and Services**
  - Individuals and organizations that develop tools for discovering and managing software assets
- **Software Consumers**
  - Individuals and organizations that install and use commercial, open source, and/or in-house developed software products

NIST IR 8060: Document Organization

- **Section 2 – SWID Tag Overview**
  - SWID Tag Types and the Software Lifecycle
  - SWID Tag Placement
  - Basic Tag Elements
  - Authenticating SWID Tags (preliminary)
- **Section 3 – Implementation Guidance for all Tag Types**
  - Authoritative vs. Non-Authoritative Tag Creators
  - Implementing <Entity> Elements
  - Implementing <Payload> and <Evidence> Elements
  - Implementing Digital Signatures (preliminary)
  - Referring to and Updating Tags
- **Section 4 – Implementation Guidance Specific to Tag Type**
  - Implementing Corpus, Primary, Patch, and Supplemental Tags
- **Section 5 – Usage Scenarios**

NIST IR 8060: Guidelines—Key Objectives

- **Enhance utility of tags for cybersecurity usage scenarios**
  - Globally-unique tag identifier usable as proxy ID for tagged product
  - Product version information furnished and allows version comparison to distinguish “before” and “after”
  - Metadata furnished for targeted search and correlation
  - Detailed file manifests furnished with cryptographic hashes
- **Clarify tag maintenance processes**
  - General updating when needed to correct errors
  - Properly reflecting patches and upgrades in tags
  - Properly linking tags to one another
  - Properly signing tags (in progress)

NIST IR 8060: Usage Scenarios—Overview

- **Minimizing Exposure to Publicly-Disclosed Software Vulnerabilities**
  - US 1 - Continuously Monitoring Software Inventory
  - US 2 - Ensuring that Products Are Properly Patched
  - US 3 - Correlating Inventory Data with Vulnerability Data to Identify Vulnerable Endpoints
  - US 4 - Discovering Vulnerabilities Due to Orphaned Software Components
- **Enforcing Organizational Software Policies**
  - US 5 - Preventing Installation of Unauthorized or Corrupted Software Products
  - US 6 - Discovering Corrupted Software and Preventing Its Execution
- **Controlling Access to Enterprise Networks**
  - US 7 - Preventing Potentially Vulnerable Endpoints from Connecting to Network Resources

Open Issues

- Patching vs. upgrading
- Implementing digital signatures
- Associating corpus tags with installation packages
- Tagging products that are accessible from a device (e.g., via network-attached storage) rather than installed on local storage
- Normalizing tag data
- Multi-language issues

Next Steps

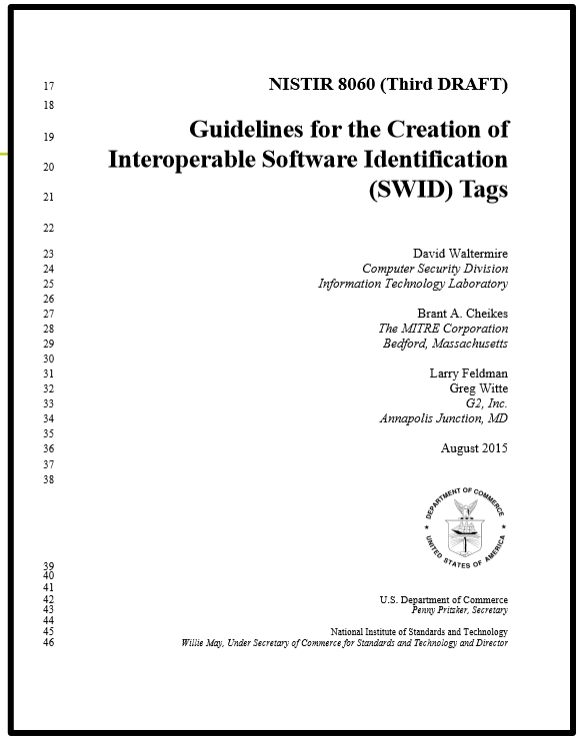
- **Finalize NIST IR 8060**
  - Address digital signatures
  - Ensure consistency with final draft of 19770-2:2015
- **Release a reference implementation for digitally signing SWID tags**
  - Simplify conformance to guidance
- **Release a reference implementation for CPE name generation**
  - Maintain interoperability with SCAP 1.x
- **Release a tag validation tool that checks conformance to IR 8060 guidelines**
  - Enable self-testing for conformance to guidance

Concluding Remarks

- **SWID tags offer many benefits to software providers, software consumers, and providers of inventory-based products and services**
- **Broad adoption is key to success—need to promote a "virtuous cycle"**
- **NIST IR 8060 is a first step—promoting awareness, providing implementation guidance and motivating usage scenarios**

You Can Help!

- **PLEASE REVIEW AND COMMENT!!**
- **E-Mail NIST IR 8060 comments to:**
  - nistir8060-comments@nist.gov



NISTIR 8060 (Third DRAFT)

Guidelines for the Creation of Interoperable Software Identification (SWID) Tags

David Waltermire
Computer Security Division
Information Technology Laboratory

Brant A. Cheikes
The MITRE Corporation
Bedford, Massachusetts

Larry Feldman
Greg Witte
G2, Inc.
Annapolis Junction, MD

August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

- **See also:**
  - http://standards.iso.org/iso/19770/-2/2015/schema.xsd
  - http://tagvault.org/standards/swid_tagstandard/
  - http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670
  - https://en.wikipedia.org/wiki/ISO/IEC_19770

MITRE