Y/IT-278

B&W Y-12 technical services LLC

Y-12 NATIONAL SECURITY COMPLEX

PRIDE Surveillance Projects Data Packaging Project

Information Package Specification Version 1.0

28 September 2009
Matthew Kelleher

Rick Shipp
Information Technology
Y-12 National Security Complex

James David Mason
SAIC

National Nuclear Security Administration
PRIDE
Product Realization Integrated Digital Enterprise

MANAGED BY
B&W Y-12, LLC
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

UCN-13672 (1-08)

Y/IT-278

PRIDE Surveillance Projects Data Packaging Project Information Package Specification Version 1.0

28 September 2009

Matthew Kelleher

Rick Shipp
Information Technology
Y-12 National Security Complex

James David Mason
SAIC

Prepared by
Babcock & Wilcox Technical Services Y-12, LLC
Management & Operating Contractor
for the
Y-12 National Security Complex
under contract DE-AC05-00OR22800
with the
U.S. Department Of Energy
National Nuclear Security Administration

ACKNOWLEDGMENTS

The authors would like to acknowledge the contributions of Rob Wilson, Richard Secrist, Monica Love, and Martin McNeil of the PRIDE Y-12 Product Characterization System Migration Project to the information package specification. They are planning to use information packages to store information they will move from Product Characterization System and they recommended several changes to the specification that will result in better information packages for their information.

This report was prepared in XML, using the "Y-12–Report" application of Arbortext developed under the *PRIDE Surveillance Reports Collaborative Authoring Project*.

TABLE OF CONTENTS

1. INTRODUCTION

This document contains a specification for a standard XML document format called an information package that can be used to store information and the context required to understand and use that information in information management systems and other types of information archives. An information package consists of packaged information, a set of information metadata that describes the packaged information, and an XML signature that protects the packaged information. The information package described in this specification was designed to be used to store Department of Energy (DOE) and National Nuclear Security Administration (NNSA) information and includes the metadata required for that information: a unique package identifier, information marking that conforms to DOE and NNSA requirements, and access control metadata. Information package metadata can also include information search terms, package history, and notes.

Packaged information can be text content, binary content, and the contents of files and other containers. A single information package can contain multiple types of information. All content not in a text form compatible with XML must be in a text encoding such as base64. Package information is protected by a digital XML signature that can be used to determine whether the information has changed since it was signed and to identify the source of the information.

This specification has been tested but has not been used to create production information packages. The authors expect that gaps and unclear requirements in this specification will be identified as this specification is used to create information packages and as information stored in information packages is used. The authors expect to issue revised versions of this specification as needed to address these issues.

1.1 SCOPE

The XML document defined in this information package specification was developed to store NNSA Nuclear Security Enterprise (NSE) product information such as bills of materials and inspection results. If it is used to package information not associated with DOE or NNSA, its structure should be modified as needed to meet the requirements associated with that information.

This specification does not specify the information that must be stored in an information package and it does not specify the format that must be used to store that information. It recommends that widely-recognized standard forms for times and binary data be used to store information where needed.

2. BACKGROUND

NNSA established the PRIDE (Product Realization Integrated Digital Environment) program to fund projects to improve the quality of digital information in the complex and to make that information available to complex users that need it. One Y-12 project funded for FY 2008 was a project to investigate a taxonomy-based search and retrieval system to serve as a single source of Y-12 information for the NSE. All Y-12 information available to system users would be identified by standardized metadata using standard terms and formatting whose meanings and definitions were consistent across the complex. These metadata would make up the information taxonomic scheme. Appropriate metadata would be developed for Y-12 information and that metadata would be stored in an index available to all Y-12 and NSE users. Each index entry would be linked to related Y-12 information. A user would locate Y-12 information by searching for appropriate metadata terms in the index then following the links to the information.

2.1 INFORMATION SEARCH REQUIREMENTS

Y-12 report Y/IT-193 *Taxonomy-Based Search and Retrieval Implementation at Y-12* documents the results of a study on whether and how taxonomic-based search and retrieval can be implemented at Y-12. It identifiedY-12 information that may be candidates for taxonomy-based search and retrieval and identified actions required to make that information available for NSE users. The report evaluated alternatives for implementing taxonomic-based search and retrieval in the Y-12 computing environment and proposed recommendations for further work.

A major finding was that the following actions must and should be taken to prepare information for taxonomy-based search and retrieval:

- **Information to be released to search users must be identified.**

  Not all Y-12 information can be released to search engine users. Some information is not ready for release, some information has restricted distribution, and some is not in an appropriate form.

- **Some information must be packaged with context information.**

  In order for information to be useful to users, it must be associated with enough context information to understand it. Without this context information, a user may not know how to use or interpret the information and it loses much of its value.

- **Information must be assigned search metadata using terms from the standard taxonomic scheme.**

  Users will search for information using these standard taxonomic metadata terms. They must be standard otherwise users will be unable to locate the information they need.

- I**nformation must have a classification/sensitivity review and appropriate markings applied.**

  DOE and NNSA require all information to have classification and sensitivity determinations and appropriate markings applied.

- **Information must be assigned standard access control metadata.**

Search engines will use this metadata along with user access authorizations to determine whether the user is allowed access to the information.

- **Information should be stored in packages such as XML documents.**

  XML has become a standard way of storing structured information. Information package XML documents can easily contain all of the information required for taxonomic-based search and retrieval: context information, search metadata, classification/sensitivity and required markings, and access control metadata.

Based on this finding, the report recommended that Y-12

- **Start preparing information by packaging it in XML files.**

PRIDE Data Packaging Project is implementing this recommendation.

Report Y/IT-193 also showed that taxonomy-based search and retrieval has other issues such as high resource requirements so it may not be implemented. These data must be made available to users, so this project assumes that data packages will be stored and made available through product information management systems and plant or NSE records management systems.

2.2 INFORMATION PREPARATION REQUIREMENTS

Information must be reviewed for release and prepared before it can be made available to external NSE users or transferred to a records management system for long-term storage. Information to be released is prepared by ensuring that all context required to understand that information is included or available, the information is appropriately marked, and the metadata used to search for and control access to the information is included. Context, markings, and metadata must be stored with the information, either as elements of a document or as part of a package that includes the information.

2.2.1 Information Release

Y-12 information systems contain information that can be released to NSE users, information for Y-12 use only, and official records that must be transferred to a records management system. Some Y-12 information is not ready for release, some information has restricted distribution, and some is not in an appropriate form. Other information does not meet the definition of records and does not need to be transferred to a records management system. Information packages can be used for all of this information, but the packages must specify the organizational limits on distribution.

2.2.2 Information Context

Y-12 technical reports, surveillance reports, procedures, forms, and other paper-based documents generally include enough information to provide required context. Some measured product data such as coordinate-measuring machine reports also have enough information to provide context to the data. Some measured product data just consist of single data points or sets of data points. Context for these data is provided by relationships to other data established when the data are stored in the information management system. If these data points were retrieved by themselves, related context would not be retrieved, and the data would be separated from its context. These data points would have limited use for the user. For

example, a set of part weights has no value if that set does not also include weight units and the identities of the weighed parts.

2.2.3 Classification Review and Marking

DOE regulations require all documents made available outside specified work groups have a current classification review and be marked according to current document marking requirements. All information made available to NSE users or transferred to a records management system may have to be reviewed to verify that they are properly classified and meet document marking requirements. These markings may include the standard admonitory notices and caveats, identity of the derivative classifier, and guidance used. When classification guidance or marking requirements change, information may have to be reviewed again and/or remarked to conform to the new requirements.

2.2.4 Search Metadata

Information made available through a information management system should have an associated set of search metadata that can be used to locate the information. These metadata should conform to NSE taxonomy and formatting standards and be stored with the information in a standard location so search engines and indexing utilities can find them. Search metadata for some information such as inspection records can be automatically generated. Search metadata for scanned documents can be extracted from the document using character recognition technology. However, this technology is unreliable and will produce metadata terms that do not conform to the taxonomy or formatting standards. For example, these documents may use technical terms that are synonyms for terms in the standard taxonomic scheme or use terms in the taxonomic scheme to mean something different than the defined meaning.

2.2.5 Access Control Metadata

Access control metadata are a set of a set of terms used to determine whether a user is allowed to know of the existence of information and the type of access that user is allowed to have to that information. This metadata must use a standard set of terms that have the same meaning throughout the NSE. An information management system would use this metadata and knowledge about the user to determine the type of access a user is allowed to have to information. These metadata may be assigned automatically or manually, but a manual review of all access control metadata may be required to verify that the original determination is complete and correct.

2.2.6 Information Packaging

Information available through an information or records management system must have associated context, markings, search metadata, and access control metadata. Context and markings must be stored with the information. Metadata must be stored with the information when that metadata is created but may be separated when the information is added to the search and retrieval system. Some information is managed as a single entity but is stored in separate places such as in separate files or database rows. This information must be presented to a user as a single package of information. Examples of how information must be packaged include:

- Data in multiple related files – An inspection result may consist of a set of files or other structured data collections. The complete set is a package, its individual files and/or structured data collections are not.
- Data stored in normalized database tables – A package can be assembled by de-normalizing the data.
- Data stored in object hierarchies – Object hierarchies are similar to normalized database tables in that relation objects identify other objects with important context information. A package can be assembled from information stored in a set of related objects.
- Drawing files – Drawing files are simple pictures of the drawings. Information describing the drawing must be included in the package.
- Scanned Paper Forms – Scanned forms are simple pictures of the forms that have not been processed using character-recognition technology. Information describing the information in the form must be added to the information package.

These packages may need to include additional context, search metadata, and access control metadata.

2.3 INFORMATION PACKAGING IN XML DOCUMENTS

XML documents can be used to store context, markings, metadata, documents, file contents, and other information in a single package. XML (Extensible Markup Language) was created by the World Wide Web Consortium (W3C) in 1998 as a language for specifying the structure of structured information. W3C is responsible for defining and managing Web standards such as HTML (Hypertext Markup Language) and cascading stylesheets, and they saw a need for a simple standardized language that can be used to specify the structure of documents presented over the Web. This simple standardized language would allow document creators to specify the structure of their documents and for Web browsers to present those documents as their authors intended.

XML is based on Standard Generalized Markup Language (SGML), a powerful but complex language that evolved out of early experiences in the late 1970s and early 1980s with generic markup languages that specify how documents are organized. SGML is an International Organization for Standardization (ISO) standard (ISO 8879:1986) and has been used to define HTML and other standard document languages. To eliminate some of the legacy complexities in SGML, the W3C created XML in the 1990s as a profile derived from SGML that would meet these design goals (from W3C):

1. XML shall be straightforwardly usable over the Internet.
2. XML shall support a wide variety of applications.
3. XML shall be compatible with SGML.
4. It shall be easy to write programs which process XML documents.
5. The number of optional features in XML is to be kept to the absolute minimum, ideally zero.
6. XML documents should be human-legible and reasonably clear.
7. The XML design should be prepared quickly.
8. The design of XML shall be formal and concise.
9. XML documents shall be easy to create.

10. Terseness in XML markup is of minimal importance.

Since the original publication of XML in 1998, the W3C has developed and release a number of additional standards based on and/or related to XML:

- XSL Transformations (XSLT) – A language for transforming XML documents from one form to another
- XSL Formatting Objects (XSL-FO) – An XML vocabulary for specifying document formatting
- XML Path Language (XPath) – A language used to access or refer to parts of an XML document. (XSLT, XSL-FO, and XPath are based on technologies developed in ISO/IEC 10179, Document Style Semantics and Specification Language [DSSSL].)
- XML Query Language (XQuery) – A language that provides flexible query facilities to extract data from XML documents.
- XML Schemas – Mechanisms to define and describe the structure, content, and to some extent semantics of XML documents.
- Document Object Model (DOM) – A standard set of objects for representing HTML and XML documents, a standard model of how these objects can be combined, and a standard interface for accessing and manipulating them.

The ISO has further extended XML in a family of standards (ISO/IEC 19757) that provide additional schema languages and tools for combining and extending schemas.

XML is widely used in industry and is strongly supported by the US National Archives and Records Administration, DOE, and NNSA. XML is supported as a native data type in Oracle release 10.2 and up, Microsoft SQLServer, and other databases. Software libraries are available to work with XML and its related languages on all significant platforms in all environments.

XML uses structures of elements with attributes to describe the contents of a document. Every element of a document is enclosed in a start tag and an end tag. The start tag has a generic identifier (text name) and can contain attributes. The end tag contains the same generic identifier as the start tag with a symbol added to identify it as the end tag. The generic identifier generally describes the contents of the element. It can be a phrase like title for a title or abstract for a paragraph that summarizes the contents of a report. Attributes consist of name-value pairs where the name is a property of the element. Attribute names and their values are text. Elements in a document are organized into a hierarchy. Elements cannot overlap – every element below its parent must be closed before the parent can be closed. The entire document is enclosed in a root element.

2.3.1 XML Benefits

Using XML to package information for information and records management systems provides several benefits. All metadata required to search for, protect, and control access to information is in the XML document that contains the information, so this information can be easily extracted by information management systems, stored in indexes, and used to control access. Information entities and context required to understand and use information are in a single XML document, so a user that receives an XML document from a query gets a complete package of information. Information stored in XML documents

can be moved to new systems or environments simply by moving the document, so it should be relatively easy to migrate information packages to new systems as old systems become obsolete.

3. INFORMATION PACKAGE REQUIREMENTS

Previous sections have described general requirements that information packages must meet to provide appropriate access control, meet DOE requirements for information marking, enable users to locate the information, and protect the information. These general requirements are expressed as specific requirements in this section along with additional requirements that must and should be met to make information packages a practical format for storing information.

Each information package requirement is listed below. With each requirement is the justification for the requirement and how that requirement is met in this specification. Further information about how the techniques used to meet these requirements are in following sections.

1. **An information package must have a unique identifier.**

   Every information package must have a unique identifier that serves as an unambiguous reference to that information package. This unique identifier is required so that calculations performed using information in information packages or actions taken based on information in information packages can be traced back to the information packages used.

   This requirement is met in this specification by providing an XML element named `<PackageIdentifier>` that contains a package identifier.

2. **The information package identifier must provide for version control.**

   Version control may be needed in situations where information already stored in information packages may be modified. For example, product inspection information may be stored in an information package as soon as it is collected. That information may subsequently be added to, corrected, approved, and have a specification exception recorded for it. The information management system may be designed to permanently save each information package version as the package is changed. Version control allows the first information package to be assigned a unique identifier that consists of a unique base identifier and a version. Each changed package would be assigned the base identifier and a new version identifier. In this way the combined package identifier would remain unique.

   This requirement is met by the `<PackageIdentifier>` element revision and instance attributes.

3. **An information package must have information markings that conform to DOE requirements**

   DOE regulations require that all information be marked as required to protect that information. If the information is classified, the markings must include the classification level and category, any required admonitory notices and caveats, and classifier information. If the information is sensitive, the markings must include all required elements for the information type.

   This requirement is met by providing an `<InformationMarking>` element whose child elements contain all required markings for classified and unclassified controlled information.

4. **An information package must have access control metadata sufficient to allow an information management system to accurately determine whether a user is allowed access to the information contained in the information package.**

   Information packages will be stored in collections such as product information management systems and databases. These collections can be expected to contain a wide variety of information. Not everyone with access to the collection will have a need to know all of the information in the collection, so each information package should include the access control information required for the system that manages the collection to determine whether a user is allowed access to the information. Information package collections will migrate to new systems as old systems are replaced. If access control information is in the information package, the new system can use that information to control access to the package.

   This requirement is met by providing an `<AccessControl>` element that contains access control information organized as name-value pairs to provide flexibility.

5. **An information package should have search terms that can be used to locate packages containing required information.**

   Information packages may be used to store a wide variety of information over a long period of time, so collections of information packages may contain a large number of packages. Some mechanism such as search terms should be used to allow users to search through these collections and extract from them only the information packages that user needs.

   This requirement is met by providing a `<SearchTerms>` element that contains `<SearchTerm>` elements that contain the search terms.

6. **Information in information packages should be stored using formats that conform to recognized standards issued by appropriate standards institutions.**

   Information packages may be stored for decades so the information in them should be stored using formats that will remain understandable for decades. Only formats that conform to recognized standards can be expected to be understandable for this length of time. Formats used by vendor software will remain understandable only as long as the vendor supports the format. Once vendor support ends, the information is likely to quickly become unreadable. A site-specific format will remain understandable only as long as the site supports it. Once site support is lost, the information becomes unreadable.

   This requirement is met by recommending standard forms for dates, times, and measurement units and a standard for encoding binary data and other information not in a form compatible with XML.

7. **Information in information packages should be protected so that changes to the information can be detected.**

   Information packages will be stored on digital media that is not 100% reliable, so the information in these packages may be damaged over time. This damage may be hard to detect

and may significantly alter the information in the package. Some mechanism for detecting this damage should be used so users can identify and handle damaged information packages appropriately.

This requirement is met by using an XML signature, a standard implementation of digital signatures for XML documents, to sign the packaged information.

8. **The information in information packages should be protected so that the source of the information can be reliably identified.**

   This provides an extra level of protection from a possible accidental mixing of valid information packages and other information packages such as test packages.

   This requirement is met by using an XML signature to sign the packaged information. The certificate that contains the public key used to decrypt the signature identifies the organization that signed the information.

9. **Information packages should have a processing history.**

   This processing history can be used to provide additional information that may help a user understand the information in the package.

   This requirement is met by including a history section in the information package.

10. **Information packages should protect the packaged information yet allow the information package metadata to be changed as needed.**

    The packaged information must be protected in such a way that changes to the packaged information can be detected and the source of the packaged information identified. However, information package metadata such as package identifier, access control, information marking, search terms, processing history, and notes should be allowed to change. The package identifier can be changed to identify successor versions. Access control and information markings can change to reflect new access control and information marking requirements. New search terms may be identified and entries added to the processing history.

    This requirement is met by signing only the packaged information. The rest of the information is not protected and can be changed at any time.

11. **Information packages must provide for optional references that can be used to identify related information packages.**

    Packaged information is often related to other information stored in separate information packages. Information packages must have function that allows information packages to refer to other information packages.

    This requirement is met by including references to other information packages in the information package metadata.

4. INFORMATION PACKAGE IDENTIFIER

Every information package must have a unique identifier that serves as an unambiguous reference to that information package. This unique identifier is required so that calculations performed using information in information packages or actions taken based on information in information packages can be traced back to the information packages used. In addition, this unique identifier can be used to

- Locate the information package in an information package collection
- Identify predecessor and successor information packages
- Identify related information packages
- Serve as the unique key that identifies the information package in a database

The `<PackageIdentifiers>` element contains the required package identifier, optional package identifiers for predecessor and successor information packages, optional package description, optional alternate identifiers for the information package or the information in the information package, and creation and modification timestamps.

4.1 UNIQUE PACKAGE IDENTIFIER

The package identifier is in a `<PackageIdentifier>` element within the `<PackageIdentifiers>` element. This element has a required `site` attribute and a required `identifier` attribute. The `site` attribute value must be a standard NSE site identifier. The `identifier` attribute value must be an alphanumeric string that is not used for any other information package identifier at the site. Together these attribute values form an information package identifier that is unique within the NSE.

Any process that generates a unique value can be used to generate the value for the `identifier` attribute. The values listed below are very likely to be unique and are acceptable values:

- Integer number that represents the system time in milliseconds plus a random 4-digit number
- Hash value generated by using a hash function such as Secure Hash Algorithm [FIPS 180-3] to generate a hash from the system name, system time, and some or all of the information in the information package
- Unique identifier assigned by Windchill PDMLink or other product information management system to the object representing the information package

4.2 VERSION CONTROL

The package identifier can include optional version control. This version control may be needed in situations where information already stored in information packages may be modified. For example, product inspection information may be stored in an information package as soon as it is collected. That information may subsequently be added to, corrected, approved, and have a specification exception recorded for it. The information management system may be designed to permanently save each information package version as the package is changed. Adding version control allows the package identifier to consist of a unique identifier that does not change and a version that can change with the combined identifier and version creating a unique package identifier.

Version control is implemented by adding an optional `revision` attribute and an optional `instance` attribute to the package identifier. A version controlled information package may use one or both of these attributes. The values of these attributes may be any alphanumeric string.

One possible way of using these attributes when information packages are stored in Windchill PDMLink is to store the value of the Windchill PDMLink revision in the package identifier `revision` attribute and the value of the Windchill PDMLink iteration in the package identifier `instance` attribute.

Version control can be implemented without using the `revision` and `instance` attributes by using the `<PredecessorIdentifier>` and `<SuccessorIdentifier>` elements to specify the order of the versions.

4.3 PREDECESSOR AND SUCCESSOR PACKAGE IDENTIFICATION

Element `<PackageIdentifiers>` has optional `<PredecessorIdentifier>` and `<SuccessorIdentifier>` elements that allow the identities of predecessor and successor information packages to be specified. These elements have the same attributes as the `<PackageIdentifier>` element and are expected to have the same values as the `<PackageIdentifier>` element in the referenced package.

4.4 PACKAGE STATUS AND DESCRIPTION

Element `<PackageIdentifiers>` has optional `<PackageStatus>` and `<PackageDescription>` elements that describe the information. A lifecycle state or other phrase describing the status of the information such as active, obsolete, or released can be placed in element `<PackageStatus>`. Element `<PackageDescription>` can contain a general text description of the information package in its element text.

4.5 ALTERNATE IDENTIFIER

Element `<PackageIdentifiers>` can have optional `<AlternateIdentifier>` elements that are used to specify alternate identifiers for the information package or the information in the information package. The `name` attribute specifies the name of the identifier and the `usedFor` attribute can have one of two values: `package` or `information`. A value of `package` means that the identifier is for the whole package and a value of `information` means the identifier is for the information in the information package. For example, if the whole information package was stored in a separate system and had an identifier in that system separate from the identifier in the `<PackageIdentifier>` element, the `<AlternateIdentifier>` element can be used to specify that other system identifier.

4.6 TIMESTAMPS

The optional `<CreatedTimestamp>` and `<ModifiedTimestamp>` elements contain a timestamp that identifies the time the information package was created or modified. The timestamp is in the element text and should conform to the timestamp format recommended in this specification.

The specification allows for only one <ModifiedTimestamp> element in <PackageIdentifiers> because this timestamp is designed to be used only to help identify the information package. If an information package history must be maintained, this history should be recorded as events in the <History> element.

5. INFORMATION MARKING

All Department of Energy classified and unclassified controlled information must be protected by marking it as required by DOE regulations. These markings warn those in possession of classified or unclassified controlled information not to release that information to persons or systems not allowed access to that information.

The `<InformationMarking>` element contains the information marking required to protect the information in the information package. If the information is classified, required markings are placed in the `<Classification>` element. If the information is unclassified controlled information, required markings are placed in the `<UnclassifiedControlled>` element.

Information packages are expected to be used to store a wide variety of classified and unclassified information. To ensure that classified information is protected, the `<Classification>` element is required and must include the classification level. If the information is unclassified, it must state that the information is unclassified. If the information is unclassified, the `<Classification>` element can be followed by one or more `<UnclassifiedControlled>` element. Each element contains markings for one type of unclassified controlled information in the package. The resulting sets of markings notify users of the classification or sensitivity of the information in the package.

The `<InformationMarking>` element is the second element in the information package after the element that contains the package identification. This placement ensures visibility when the file is viewed. The first element contains the package unique identifier. This identifier is considered part of the markings when the information in the package is considered accountable.

5.1 CLASSIFIED INFORMATION

DOE manual 470.4-4A issued in January 2009 [DOE M 470.4-4A] specifies markings required for classified documents and material. Document marking requirements assume the document is a traditional paper document such as a letter or report. Material markings require the existence of a drawing that contains required marking information. There are no requirements for other information formats such as XML documents. The only requirement is [DOE M 470.4-4A]:

> *Classified matter, regardless of date or agency of origin, must be marked to indicate at least the classification level and category (if RD or FRD).*

The classified information marking requirements in this specification are based on the document marking requirements in 470.4-4A.

5.1.1 Classification Level and Category

The `<Level>` element specifies the highest classification level of the information in the information package and is required. Its element text must be one of these four values:

- `Top Secret`
- `Secret`
- `Confidential`

- `Unclassified`

The capitalization used in the level is required because it is the capitalization used for these words in DOE manual 470.4-4A. To ensure that software can recognize the value, only one blank must separate the words in `Top Secret`.

If the information in the information package is unclassified, this element must be present and contain `Unclassified` as its element text. The presence of `Unclassified` demonstrates to users that the information in the information package received a classification review when it was originated.

The `<Category>` element specifies the highest classification category of the information in the information package. Its element text must be one of these three values:

- `Restricted Data`
- `Formerly Restricted Data`
- `National Security Information`

Only one blank must separate the words in the category names. The capitalization used in the category is required because it is the capitalization used for these words in DOE manual 470.4-4A.

The classification category is required if the classification category is Restricted Data or Formerly Restricted Data. It is optional if the classification category is National Security Information. It must not be present if the classification level is Unclassified.

5.1.2 Caveats and Special Control Markings

Caveats and special control markings are placed on documents to identify special handling or dissemination requirements or to assist in describing the type of information involved or who distributed or originated the information. An information package caveat is placed in the element text of a `<Caveat>` element and a special control marking is placed in the element text of a `<SpecialControlMarking>` element.

The contents of each element are based on the requirements for the information in the information package. If a caveat or special control marking is not required, the corresponding element should not be present.

5.1.3 Admonishment

If the information in the information package is `Restricted Data` or `Formerly Restricted Data`, the corresponding admonishment is placed in the element text of the `<Admonishment>` element. Otherwise this element should not be present.

5.1.4 Document Title, Originating Organization and Date

The information package can be given a formal document title or subject that describes the contents of the information package. This title or subject is optional, placed in the `<Title>` element text, and must be marked as required by DOE manual 470.4-4A.

DOE manual 470.4-4A has a requirement that states the name and address of the organization responsible for preparing a classified document and the date of preparation must appear on the first page of the classified document. The organization name is placed in the `<OrganizationName>` element and the

organization address is placed in the <OrganizationAddress> element text. The organization name and address are text strings with parts separated by commas or other delimiters as necessary.

If the <CreatedTimestamp> or <ModifiedTimestamp> elements are not present in the <PackageIdentifiers> element, the <DocumentDate> element can be used to specify a document preparation date. This date can be in any appropriate date format. Otherwise the date in the <CreatedTimestamp> or <ModifiedTimestamp> serves as the document date. The document date does not have to conform to the date and time formats recommended by this specification.

5.1.5 Classification Determination

The information on how the classification was determined is placed in the <ClassifiedBy>, <DerivedFrom>, and <DeclassifyOn> elements. The tag names of these elements are based on the corresponding classifier markings lines required on documents by DOE manuals 470.4-4A and 475.1-1B. The classifier identification is placed in the <ClassifiedBy> element text, the source of the classification guidance is placed in the <DerivedFrom> element text, and for information packages that contain only National Security Information, declassification information is placed in the <DeclassifyOn> element text. Formats and contents of the element text of these elements are specified by DOE manuals 470.4-4A and 475.1-1B.

This specification has element <DateReviewed> that specifies the date the document was reviewed. DOE manuals 470.4-4A and 475.1-1B assume that the document date is the date reviewed. However, information packages may not be formally reviewed until long after the packages are created. Furthermore, they may be changed after the formal review is performed without another classification review being performed. The <DateReviewed> element text contains the most recent date a formal classification review was performed on the information in the information package. A user can use this information to judge whether this classification review is valid for the information in the information package. This date can be in any standard date format.

5.1.6 Additional Information

The <AdditionalInformation> element is optional and can be used to provide additional information about the classification decision. The following are examples of additional information that can be stored using this element:

- Statement “Derivative Declassifier review required prior to declassification” required when the information package contains only NSI information.
- Sources used to make the classification determination when multiple sources are used
- Classification level and category matrix when the information package contains information in multiple classification categories
- Additional information about the classification process used when an automated process is used to make the classification determination

Each independent statement should be in a separate <AdditionalInformation> element. If additional information is not required, this element should not be present.

5.2 UNCLASSIFIED CONTROLLED INFORMATION

Unclassified controlled information (UCI) is information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U.S. Government. Governmental interests are those related, but not limited to, the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law-enforcement information as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens. In addition, other unclassified sensitive information is information that, based on a determination by competent authority (e.g., information owners), may require mandatory protection because of statutory or regulatory restrictions or may require a degree of discretionary protection because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect national, Department of Energy/National Nuclear Security Administration (DOE/NNSA), or DOE contractor interests. [Y19-206]

These are the types of unclassified controlled information that may be present at the Y-12 National Security Complex:

- Unclassified Controlled Nuclear Information (UCNI)
- Export Controlled Information (ECI)
- Naval Nuclear Propulsion Information (NNPI)
- Safeguards Information (SI)
- Sensitive Nuclear Technology (SNT)
- Official Use Only (OUO)
- Applied Technology (AT)
- Cooperative Research and Development Agreement (CRADA) information
- Confidential/Foreign Government Information–Modified Handling (C/FGI-MOD)
- Privacy Act information
- Proprietary Information
- Company-owned information

Each of these types of unclassified controlled information has its own marking requirements. An information package can contain more than one of these unclassified controlled information types. When it does, the required markings for each type present must be included in the information marking.

The `<UnclassifiedControlled>` element is designed to be used for each of these unclassified controlled information types. One `<UnclassifiedControlled>` element must be present in the `<InformationMarking>` element for each type of unclassified information present. This element represents one of these information types and contains child elements that contain required admonitory markings and other required information.

The sections below describe `<UnclassifiedControlled>` child elements and then show how they are used to protect two common types of unclassified controlled information: Unclassified Controlled

Nuclear Information (UCNI) and Official Use Only (OUO) information. Marking and other requirements for other types of unclassified controlled information are described in an appendix.

5.2.1 Element Descriptions

The `<UnclassifiedControlled>` element contains the set of child elements required to specify the controlled information type, present the required admonishment statement, and to provide additional information for certain controlled information types. These elements are listed below and described in the rest of this section.

- `<AdditionalInformation>`
- `<Admonishment>`
- `<Caveat>`
- `<ClassifiedBy>`
- `<DateReviewed>`
- `<DerivedFrom>`
- `<Guidance>`
- `<GuidanceUsed>`
- `<NameOrganization>`
- `<Reviewer>`
- `<ReviewingOfficial>`
- `<Type>`

Certain unclassified controlled information types require additional labeled information such as the identity of the person or entity that determined the unclassified controlled information type or the guidance used in that determination. The element tag names are designed to match as closely as possible the labels used in the markings. In some cases elements with different tag names are used to represent basically the same information. This specification assumes that the information marking for an unclassified controlled information type will use the element with the tag name that is the closest match to the label specified in the information type marking requirements.

If information in the information package is a controlled type, the `<Type>` element contains the name of the controlled information type and must be one of these values:

- `Unclassified Controlled Nuclear Information`
- `Export Controlled Information`
- `Naval Nuclear Propulsion Information`
- `Safeguards Information`
- `Sensitive Nuclear Technology`
- `Official Use Only`
- `Applied Technology`
- `Cooperative Research and Development Agreement`
- `Confidential/Foreign Government Information-Modified Handling`
- `Privacy Act Information`

- Proprietary Information
- Contractor Information

Only one blank must separate the words in the type name. If the information is not controlled, the <Type> element must contain "Not Controlled".

The <Admonishment> element contains the admonishment text specified by the information marking requirement. These marking requirements specify the capitalization to be used in the admonishment text. This capitalization must be used in the text in the information package.

Elements <NameOrganization>, <ReviewingOfficial>, and <Reviewer> contain the identity of the person or entity that determined the unclassified controlled information type.

Element <DateReviewed> contains the date of the unclassified controlled information type was determined. This date does not have to conform to the recommended date formats and can be in any acceptable format.

The guidance used to make a determination is entered in the element text of the <Guidance> and <GuidanceUsed> elements. The content of these elements is specified by the requirements of the information type.

Element <Caveat> contains any caveat statements required to properly mark the information.

Elements <ClassifiedBy> and <DerivedFrom> identify the classifier and guidance used to mark Confidential/Foreign Government Information–Modified Handling information.

Element <AdditionalInformation> provides additional information about the marking.

5.2.2 Unclassified Controlled Nuclear Information (UCNI)

UCNI is unclassified government information that is prohibited from unauthorized dissemination under Section 148 of the Atomic Energy Act and further defined in Title 10, Code of Federal Regulations, Part 73. It includes the following information:

- Design of production or utilization of facilities related to atomic energy defense programs.
- Design-related operational information concerning the production, processing, or utilization of nuclear material for atomic energy defense programs.
- Physical security measures for the protection of production or utilization facilities related to atomic energy defense programs.

If the information package contains UCNI information, the package must have an <UnclassifiedControlled> element with the UCNI admonishment and reviewing official information.

The <Admonishment> element must be present and contain this element text:

Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).

Elements <ReviewingOfficial> and <GuidanceUsed> must be present and contain the information required for the reviewing official and guidance used lines by DOE manual 471.1-1. Element <DateReviewed> contains the review date.

If the information requires a dissemination controlled marking, the following text is placed in the <Caveat> element:

DISSEMINATION CONTROLLED Distribution authorized to DOE and DOE contractors only. Other requests shall be approved by the cognizant DOE program office, which is (office name), before release.

The (office name) text is replaced by the name of the DOE program office.

5.2.3 Official Use Only (OUO) Information

Official Use Only information is information that is unclassified and meets both of the following criteria [DOE M 471.3-1]:

- Have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities.
- Fall under at least one of eight Freedom of Information Act (FOIA) exemptions (exemptions 2 through 9).

If the information package contains OUO information, the `<Admonishment>` element must be present and contain:

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: (number and category) Department of Energy review required before public release.

The (number and category) text must be replaced by an OUO exemption number and text listed in DOE manual 471.3-1 or its successors. The name and organization of the person that made the determination is placed in the `<NameOrganization>` element text, the date the determination was made is placed in the `<DateReviewed>` element text, and the guidance used (if any) is placed in the `<Guidance>` element text.

5.3 DEFAULT CLASSIFICATION AND CONTROLLED INFORMATION DETERMINATIONS

Much of the information expected to be stored in information packages at Y-12 was collected using automated processes and stored directly in a product information management system. The process did not route the information to a derivative classifier so it never received a derivative classifier review. The information was assigned by default the highest classification level and category that the systems that created and stored it were authorized to process.

To identify information that never received a derivative classification review, the `<InformationMarking>` element has an optional attribute named `default` that can have a value of `yes` or `no`. If default is present and has a value of yes, the information package was assigned a default classification or controlled information type.

If the information is classified, the `<Level>` element must be present and contain the default classification level. If the default classification category is Restricted Data or Formerly Restricted Data, the `<Category>` element must be present and contain the classification category and the `<Admonishment>` element must be present and contain the appropriate admonishment. Any required caveats must also be present. An `<UnclassifiedControlled>` element must not be present.

If the information is unclassified, element `<Classification>` and its child `<Level>` element must be present and `<Level>` must contain `Unclassified`. If the information in the information package is not a controlled type, an `<UnclassifiedControlled>` element must be present and contain `Not Controlled`. Otherwise an `<UnclassifiedControlled>` element must be present for each type of controlled information present in the information package.

The `<AdditionalInformation>` element may be used to record additional information about how the default classification level, classification category, and controlled information type were determined.

6. ACCESS CONTROL

The access control element provides an information management system with the information required to determine whether the system should allow or deny a user or application access to the information in the information package. An information management system is expected to get the information attributes associated with the information package directly from the information package or from a separate set of metadata created from the information attributes when the information package was stored. The information management system is expected to compare the information attributes obtained from the information package with access control rules that determine whether the user or application has access. If the access control rules allow access, access is granted; otherwise it is denied.

This information package specification cannot assume in advance the information attributes that may be important to controlling access to the information package. Furthermore, required information attributes may change over time. This information package specification also assumes that information in other parts of the document is not repeated. For example, information classification level and category and unclassified controlled information type are already in the `<InformationMarking>` element and do not need to be repeated.

The most flexible design for information attributes that meets above needs is the name-value pair design. Name-value pairs are implemented as an `<InfoAttribute>` element with the name specified by an optional name attribute and the value in the element text. These elements are contained within an `<AccessControl>` element. Any number of `<InfoAttribute>` elements can be included in the `<AccessControl>` element when the package is created and new elements can be added or existing elements modified or deleted as required over time.

The following example shows what `<AccessControl>` might contain if the information in the package was inspection data for the fictitious W00 program. This access control element would allow access to persons involved in the W00 program and to inspection auditors:

```
<AccessControl>
    <InfoAttribute name=”program”>W00</InfoAttribute>
    <InfoAttribute name=”role”>auditor</InfoAttribute>
</AccessControl>
```

The system that controls access to the information package would have the final say on whether access was granted.

7. SEARCH TERMS

This information package specification does not specify the organization or contents of the packaged information. It simply states that packaged information is contained in the <PackageInfo> element text. A user using an information management system or database that provides users with the capability to search XML elements and attributes can use these capabilities to locate information packages that contain specific information. However, if that user does not exactly specify in the search the elements that contain the search information, the search will fail. To specify the exact elements, a user must know the detailed structure of all information packages being searched.

The information package can contain an element named <SearchTerms> that contains a set of search terms that describe the information in the information package. Placing all search terms in this single location makes it easy for users searching for information to specify the locations of the search terms in all information packages being searched.

All search terms are stored in <SearchTerm> elements in the <SearchTerms> element text. The <SearchTerms> element can be empty or can contain as many <SearchTerm> elements as needed to enable users to locate information in the information package.

Each <SearchTerm> element contains the search term in its element text and optional attributes that specify the name of the search term and the units of measure used for the search term. These attributes allow the user to further limit the scope of the search for the search terms.

8. DOCUMENTATION

Information packages have elements that allow users to add references that identify related information packages, add information about the history of the information package or the information in the information package, and add general notes about the information package and its information.

8.1 INFORMATION PACKAGE REFERENCES

The <References> element allows users to add <Reference> elements each of which identifies another information package related in some way to the package with the <Reference> element. The attributes of the <Reference> element are the same as the attributes of the <PackageIdentifier> element and must contain the same values as the <PackageIdentifier> element in the referenced information package. The <PackageIdentifier> element text contains a text description of the relationship.

8.2 INFORMATION PACKAGE AND INFORMATION HISTORY

The <History> element contains documentation of the events in the history of the information package or its information. The events are in order in the <History> element from oldest to newest. Each <Event> element contains the description of the event and these attributes that describe the source and consequences of the event:

- name – Person or program name
- employeeId – Employee identifier such as employee number (if known)
- site – Site identifier
- time – Date and time of the event in standard format.
- packageInfoChanged – Set to “yes” if the signed contents were changed, empty or “no” otherwise

Following is an example of a history:

```
<History> element that
  contains a single event:
  <Event name="A. User" employeeId="012345"
    site="Y-12" time="2009-03-17 13:58:03.123-400"
    packageInfoChanged=”yes”>
      Package created
  </Event>
</History>
```

8.3 NOTES

A <Notes> element allows users to add additional information to the information package about the package or the information in the package. Examples of appropriate notes include:

- Source of the information
- Quality of the information
- Reason the information package was modified

These notes are placed in the element text of <Note> elements in the <Notes> element text. These notes should be in chronological order with the oldest first. Each <Note> element contains these four attributes that describe the source of the note:

- name – Person or program name
- employeeId – Employee identifier such as employee number (if known)
- site – Site identifier
- time – Date and time of the event in standard format.

Following is an example of the use of the <Notes> element:

```
<Notes>
  <Note name="A. User" employeeId="012345"
    site="Y-12" time="2009-03-17 13:58:03.123-400">
      This is a note.
  </Note>
</Notes>
```

9. PACKAGE INFORMATION

The packaged information in the information package is stored in an XML document structure that has the <PackageInfo> element as its root. This specification does not specify the structure or form of the information in the elements below <PackageInfo>. It has recommendations for formats for information stored in the information structure and it specifies the XML signature elements required to identify the source of the information and whether it has been changed.

9.1 RECOMMENDED DATE AND TIME FORMATS

International Organization for Standardization standard 8601 [ISO 8601] specifies standard numerical representations for dates, times and combined dates and times. A note submitted to the World Wide Web Consortium recommended that a subset of these formats sufficient to satisfy most requirements be defined and used in web applications [W3C Datetime]. The recommendations in this note provide a good set of standards for dates and times in information packages. The following discussion was extracted from that document:

The formats are as follows. Exactly the components shown here must be present, with exactly this punctuation. Note that the "T" appears literally in the string, to indicate the beginning of the time component, as specified in ISO 8601.

Year:
YYYY (e.g., "1997")
Year and month:
YYYY-MM (e.g., "1997-07")
Complete date:
YYYY-MM-DD (e.g., "1997-07-16")
Complete date plus hours and minutes:
YYYY-MM-DDThh:mmTZD (e.g., "1997-07-16T19:20+01:00")
Complete date plus hours, minutes and seconds:
YYYY-MM-DDThh:mm:ssTZD (e.g., "1997-07-16T19:20:30+01:00")
Complete date plus hours, minutes, seconds and a decimal fraction of a second
YYYY-MM-DDThh:mm:ss.sTZD (e.g., "1997-07-16T19:20:30.45+01:00")

where:

```
YYYY = four-digit year
MM   = two-digit month (01=January,   etc.)
DD   = two-digit day of month (01 through   31)
hh   = two digits of hour (00 through 23)   (am/pm NOT allowed)
mm   = two digits of minute (00 through   59)
ss   = two digits of second (00 through   59)
s    = one or more digits representing a decimal fraction of a second
TZD = time zone designator (Z or +hh:mm or   -hh:mm)
```

This profile defines two ways of handling time zone offsets:

1. Times are expressed in UTC (Coordinated Universal Time), with a special UTC designator ("Z").
2. Times are expressed in local time, together with a time zone offset in hours and minutes. A time zone offset of "+hh:mm" indicates that the date/time uses a local time zone which is "hh" hours

and "mm" minutes ahead of UTC. A time zone offset of "-hh:mm" indicates that the date/time uses a local time zone which is "hh" hours and "mm" minutes behind UTC.

The "T" character between the date and time makes it harder for a human to separate the date from the time. An acceptable alternative to the above formats is to replace the "T" character with a single blank character.

An alternative to the numeric time zone format +/- hh:mm is the +/- hhmm time zone format specified in RFC 822 [RFC 822]. This format is currently used for electronic mail and other internet-related services. This time zone format will probably be the preferred format for information packages generated by software written in the Java language because it is much easier to generate a time zone in this format using Java than in the above format.

If another date or time format is used, it should clearly identify whether it is based on coordinated universal time (UTC, also known as Greenwich Mean Time or GMT) or is a local time. If it is a local time, the difference between the local time and UTC should be specified. It can be specified using a time zone such as Eastern Daylight Time (EDT) or by an offset from UTC such as -04:00 (EDT) or -05:00 (Eastern Standard Time).

9.2 RECOMMENDED MEASUREMENT UNIT ABBREVIATIONS

The abbreviations used for measurement units for units defined by the International System of Units (SI) should use the abbreviations defined by *The International System of Units* [SI].

The abbreviations used for traditional US units of measurement such as inch, pound, or gallon should follow the conventions specified in National Institute for Standards and Technology (NIST) handbook 44 [NIST 44].

9.3 RECOMMENDED BINARY FILE ENCODING

Internet Engineering Task Force Request for Comments 4648 *The Base16, Base32, and Base64 Data Encodings* [RFC 4648] specifies standard encodings for converting binary content to and from a text encoding suitable for use in XML documents. The base64 encoding defined in this RFC should be used to convert binary data and other data not compatible with XML to a text-based encoding that can be stored in XML documents. When converting a base64 text encoding to binary data, characters outside the base encoding alphabet must be ignored when interpreting data. The encoded text may include white space characters such as spaces, tabs, carriage returns, and line feeds when required to make the encoding easier to read in an XML document.

10. XML SIGNATURES

A digital signature implemented as an XML signature is used to detect changes to the contents of the packaged information and to confirm the origin of the information. A digital signature is described in National Institute of Standard and Technology (NIST) Federal Information Processing Standards (FIPS) *Digital Signature Standard* (DSS) as follows [FIPS 186-3]:

"A digital signature is an electronic analogue of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data). These assurances may be obtained whether the data was received in a transmission or retrieved from storage."

W3C *XML Signature* recommendation [XMLDSIG 2002] and its second edition [XMLDSIG 2008] specify XML syntax and processing rules for creating and representing digital signatures in XML documents. These signature recommendations are an implementation of the NIST FIPS 186-3 *Digital Signature Standard* for XML documents.

Contents of the`<PackageInfo>` element are protected by a digital signature that conforms to the first W3C XML signature recommendation [XMLDSIG 2002], the second edition of that recommendation [XMLDSIG 2008], or a subsequent edition, revision, or replacement of that recommendation. The revision or edition of the standard used will be identified in the signature as required by the standard.

10.1 DIGITAL SIGNATURES

A digital signature is a string of bits that represents both the signed content and the signer. The signed content is represented by a message digest created by using a hash function to transform the content to a string of bits. This string of bits is encrypted by the signer using a standard encryption algorithm and key known to the signer. The bit string generated by the encryption algorithm is the digital signature. When public key cryptography is used, the signer's private key is used to encrypt the bit string.

The signature can be verified by using the same hash function to create a message digest from the signed content. When the signer and verifier share a secret key, the verifier uses the same encryption algorithm and key to decrypt the message digest. When public key cryptography is used, the verifier uses the signer's public key to decrypt the message digest. If message digest calculated by the verifier matches the message digest in the message, the signatures match and the verifier knows that the signed content was signed by the signer and has not changed since the signature was calculated.

Digital signatures are secure because of the characteristics of the hash and encryption functions used to create them. A hash function algorithm is considered secure if, for a given algorithm, it is computationally infeasible (1) to find a message that corresponds to a given message digest, or (2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest [FIPS 180-3]. The Secure Hash Algorithm (SHA) specified by [FIPS 180-3] and used in XML signatures meets these requirements.

The message digest is encrypted by the signer to show that the signer had access to the key required to encrypt it. If a secure encryption algorithm was used, it is computationally infeasible to create the appropriate signature bit string without knowing the encryption key. Since encryption is reversible, every unique encrypted bit string has one corresponding decrypted bit string and vice versa. Together these characteristics ensure that, if the decrypted signed message digest in the message corresponds to the message digest calculated from the message, the signer had access to the key used to sign it and the message has not changed since it was signed.

A message can be signed using a shared secret key or by using public and private keys. A shared secret key is shared by the signer, the verifier, and possibly by others. The key must be protected from unauthorized users and uses and it must be securely preserved for the life of the information packages it was used to sign. These characteristics make it impractical to use shared secret keys to sign information packages.

Public-key cryptography uses asymmetric key algorithms instead of the symmetric key algorithms used with shared secret keys. Asymmetric key algorithms use a pair of keys instead of the single shared key used in symmetric algorithms. If the two keys are designated *k1* and *k2*, then using the appropriate asymmetric key algorithm, a message encrypted using *k1* must be decrypted using *k2* and a message encrypted using *k2* must be decrypted using *k1*. Furthermore, it is computationally infeasible to use one of the keys in a key pair to determine the other key. This allows a user to keep key *k1* private and allow key *k2* to be publicly known. A person can digitally sign a message by using a private key to encrypt the message digest. A second person can verify the digital signature by decrypting the signed message digest using the corresponding public key, computing the message digest, and comparing the two digests. If they match, a person in possession of the private key signed the message and it has not changed since it was signed.

These characteristics allow digital signatures to be used for these three purposes:

- Detect unauthorized modifications to signed information
- Authenticate the identity of the signer
- Prevent the signer from later repudiating the signature and signed information

If a message is altered in any way without signing the information again, the secure hash algorithm will calculate a significantly different message digest and an attempt to verify the signature will fail. A verification of a digital signature using a public-key cryptography public key proves that the corresponding private key was used to sign the message and that the message came from a source that knew the private key.

10.2 DIGITAL SIGNATURES IN INFORMATION PACKAGES

Digital signatures are used in information packages primarily to detect changes to the protected information stored in the packages. These changes are most likely to occur as a result of accidental damage to the information. Such damage can be the result of transmission errors when moving an information package or from damage to the medium used to store the information package.

Digital signatures also allow analysts using the information in the information packages to verify that the information in the package is the same information that was stored in the package when it

was created. The digital signature allows the analyst to eliminate information from an analysis where digital signatures show that the information package that contains the information has changed and the information may not be valid.

The digital signature also authenticates the origin of the information. This factor is important only if the information in an information package may be deliberately modified or if the origin of the information is uncertain. Every digital signature consists of a message digest encrypted using a private key. The corresponding public key is encoded in a certificate that is included in the digital signature. Each certificate has an associated value called a fingerprint that is unique to the certificate. If the fingerprints calculated from two certificates are identical, the certificates are identical. If the signed contents of an information package were deliberately altered and were signed, the signing certificate will be different unless the signer had access to the private key used to sign the original signed contents. This different certificate will be revealed by comparing its fingerprint to the fingerprint obtained from certificates in valid information packages. Likewise, the source of an information package can be determined by comparing the fingerprint of its certificate to the fingerprints of certificates from information packages with known sources.

10.3 XML SIGNATURES

The XML signature standards [XMLDSIG 2002, XMLDSIG 2008] and the references specified in these standards describe the digital signature standard for XML documents. These specifications have been implemented in a number of software packages. This information package specification assumes that a software package implementation that conforms to these standards will be used to sign the signed contents of information packages, so a discussion of how digital signatures are created is not appropriate. The XML signature specifications do specify a number of options and these options are discussed in this section.

The XML signature implemented in this specification has this implementation:

```
<Signature xmlns="XML signature namespace URL">
  <SignedInfo>
      <CanonicalizationMethod
      Algorithm="canonicalization method URL"/>
      <SignatureMethod Algorithm="signature method URL"/>
      <Reference URI="#SignedContents">
        <Transforms>
          <Transform
            Algorithm="XML signature enveloped signature URL "/>
        </Transforms>
        <DigestMethod Algorithm="XML signature digest method URL"/>
        <DigestValue>Dhg ... XU=</DigestValue>
      </Reference>
  </SignedInfo>
  <SignatureValue>Dc ... Oc=</SignatureValue>
  <KeyInfo>
     <X509Data>
       <X509SubjectName>CN= ... ,C=US</X509SubjectName>
       <X509Certificate>MIIE ... Zrq8=</X509Certificate>
     </X509Data>
  </KeyInfo>
```

```
</Signature>
```

These elements have the following meanings:

Tag Name	Element Description
`Signature`	Container for the XML signature. The `xmlns` attribute sets the namespace to the XML signature namespace to ensure that child elements are considered XML signature elements and not elements in other namespaces.
`SignedInfo`	Container for the information to be signed. Its child elements specify the message digest and how it is created and signed.
`CanonicalizationMethod`	The method used to convert the signed contents to its canonical form.
`SignatureMethod`	The name that represents all methods used to create the signature. It includes the name of the digest method and the name of the method used to sign the digest value.
`Reference`	Identifies the information to be signed. Its URI attribute must be a document fragment that references the value of the id attribute of the signed element, either the `<PackageInfo>` element or one of its child elements.
`Transforms`	Container for `<Transform>` elements.
`Transform`	Specifies how the signed information element is processed to create the signature.
`DigestMethod`	The method used to calculate the message digest from the signed contents.
`DigestValue`	The message digest calculated from the signed contents in base64 format.
`SignatureValue`	The message digest encrypted using the private key in base64 format.
`KeyInfo`	Container for the certificate that contains the public key used to decrypt the message digest.
`X509Data`	Container for the certificate.
`X509SubjectName`	Certificate name.
`X509Certificate`	Certificate in base64 format.

The `<CanonicalizationMethod>` element Algorithm attribute defines the method used to transform the contents of the `<SignedInfo>` element to a standard form. Secure Hash Algorithm and other message digest algorithms calculate their digests from all of the information provided them, so a message digest value calculated from an XML document fragment will depend on the document contents and structure. W3C has issued recommendation Canonical XML versions 1.0 and 1.1 that specify a standard structure for XML documents. The goal of these specifications are to establish a method for determining whether two XML documents are identical, or whether an application has not changed a document, except for transformations permitted by XML 1.0 and Namespaces in XML 1.0. [C14N10, C14N11].

Element `<SignatureMethod>` defines the combination of the message digest algorithm used to create a message digest of the contents of the `<SignedInfo>` element and the algorithm used to encrypt it to create the signature value. These combinations use Secure Hash Algorithm to create the message digests but differ in how the message digest is signed:

- HMAC-SHA-1
- DSAwithSHA-1

- RSAwithSHA-1

HMAC-SHA-1 uses a message authentication code encrypted using a shared secret key to create the signature. A shared secret key is not likely to be preserved over time, so this alternative is not considered acceptable.

DSAwithSHA-1 and RSAwithSHA-1 both use public key encryption to encrypt the message digest creating the signature. DSAwithSHA-1 uses the Digital Security Algorithm defined in [FIPS 186-3] and RSAwithSHA-1 uses the RSA algorithm defined in IETF RFC 2437. Algorithm DSAwithSHA-1 is required and RSAwithSHA-1 is recommended. Information packages will use DSA-based algorithms both because they are required and because it is a Federal standard.

The Java software used to sign the information packages used to develop this specification automatically convert the signed packaged information to a canonical form before calculating the signature. This signed package information can change as long as the change does not significantly alter the meaning of the signed contents and the signature will still be valid. For example, the order of attributes in an element is not significant in XML so it can change without invalidating the signature. Any change that alters the meaning of the signed package information such as adding or deleting elements or attributes or changing attribute or element text will invalidate the signature.

10.4 SECURITY ISSUES

The XML Signature standard specifies that secure hash algorithm SHA-1 be used to compute the message digests. However, SHA-1 is no longer considered acceptable by NIST for protecting important sensitive unclassified information. Stronger versions of SHA are available and must be used. However, until these stronger versions become part of the XML Signature recommendation, SHA-1 will be used to compute the message digests for information packages. The risks of using SHA-1 are low in this case because a malefactor is unlikely to benefit from altering an information package. The primary threat to information packages is accidental damage, and SHA-1 is capable of detecting this.

When computing a DSA public-private key pair, the key bit length must be either 1024 or 2048 [FIPS 183-3].

11. NAMESPACES

Every element in an XML document must have a unique definition. It can be defined only once in the schema and has the same attribute definitions and element text meaning everywhere it is used in the document. However, XML documents are designed to be composed of XML structures obtained from different sources and used for different purposes. These sources can have elements with the same names and completely different definitions. Placing these conflicting elements in a single XML document is prohibited by the XML standard. To avoid these element name conflicts, W3C added namespaces to the XML standard.

An element is placed in a namespace by adding a prefix to the element tag name that is assigned to the namespace. Each namespace prefix is bound to a uniform resource identifier (URI). When a prefix is added to an element name, the complete name of the element becomes the element tag name plus the URI. This means that two elements in different namespaces with the same tag name have different names in XML and can be in the same XML document.

For example, the information package specification has a conflict between the `<Reference>` element that is a child of the `<References>` element and the `<Reference>` element that is part of the XML signature. XML Signature elements are in a namespace so the two elements can appear in a valid XML document. In the XML Signature specification the `<Signature>` element and all elements below it are assigned to the XML Signature namespace. Prefixes are not used for these elements in the XML Signature specification because their namespace is inherited from the `<Signature>` element. The recommended prefix for XML Signature elements is `ds:` and this prefix is used for all XML Signature elements in this specification and in document type definition files developed for this specification.

This namespace URI has been established for the information package elements defined in this specification:

```
xmlns:ip="urn:x-y12:InfoPackage"
```

This namespace corresponds to the uniform resource name (URN) syntax in RFC 2141 [RFC 2141] and the uniform resource names (URN) namespace definition mechanisms described in RFC 3406 [RFC 3406]. The URN namespace `x-y12` defines an internal namespace not registered with the Internet Assigned Numbers Authority (IANA). It is not guaranteed to be unique but a conflict is unlikely. In the examples used in this specification and in the document type definition files developed for this specification, the prefix `ip:` is used for all information package elements defined by this specification.

This specification recommends that child elements of the `<PackageInfo>` element that contain packaged information should use a URN namespace that starts with `urn:x-` to ensure that all elements have unique definitions. URN namespaces starting with an `x-` are considered internal or experimental and are not regulated by IANA.

12. INFORMATION PACKAGE SPECIFICATION

An information package is an XML document that meets the requirements for an information package described in section 3. It consists of a document root element and six child elements to the document root element that contain the information package metadata. These metadata consist of the package identifier, information marking, access control, search, annotations, and other information required in an information package. The seventh element contains the packaged information.

The names of the elements listed do not include a namespace prefix such as `ip:`. This specification recommends that a namespace prefix such as `ip:` be used when the elements are included in an information package.

12.1 ELEMENT `<InfoPackage>`

This element is the document root element of the information package document. It has this definition:

Tag Name	Element Description
`InfoPackage`	Document root element for the information package. Its element text contains the elements listed below in the order listed: one `<PackageIdentifiers>` element one `<InformationMarking>`element one `<AccessControl>`element zero or one `<SearchTerms>`elements zero or one `<History>`elements zero or one `<Notes>`elements zero or one `<References>`elements one `<PackageInfo>`element

Element `<InfoPackage>` has two attributes that describe the information package:

Attribute	Attribute Description
`xmlns:ip`	Specifies the name the `ip` namespace prefix is bound to. It is optional and if present must have the value `urn:x-y12:InfoPackage`
`version`	Specifies the information package version. It is optional and if present must have the value `1.0`

If the `xmlns:ip` attribute is present, the prefix it specifies must be added to the names of all `InfoPackage` child elements and their attributes.

The `version` attribute specifies the version of the information package specification used to create the information package. The value of the `version` attribute tells users and software the elements defined

by the information package specification that may be present and how they may be structured. The version of the packaged information is specified in <PackageIdentifiers> child elements.

12.2 ELEMENT <PackageIdentifiers>

Element <PackageIdentifiers> contains the information used to identify the information package. Its elements specify a unique identifier for the information package and the identifier of the predecessor and/or successor information packages if the information package is in a series. Its elements also specify a package description, alternate identifiers for the information package or the information in the information package, and timestamps that record when the information package was created and modified.

Element <PackageIdentifiers> has this definition:

Tag Name	Element Description
PackageIdentifiers	Contains the information used to identify the information package and the information in the information package. Element body has these elements in this order: one <PackageIdentifier> element zero or one <PredecessorIdentifier> elements zero or one <SuccessorIdentifier> elements zero or one <PackageDescription> elements zero or one <PackageStatus> elements zero or more <AlternateIdentifier> elements zero or one <CreatedTimestamp> elements zero or one <ModifiedTimestamp> elements

This element has no attributes. The required <PackageIdentifer> element must be first and be followed by the optional elements in the order specified above.

12.2.1 Elements <PackageIdentifier>, <PredecessorIdentifier>, and <SuccessorIdentifier>

Element <PackageIdentifer> identifies the information package. When the information package is one of a series of information packages such as when versioning is used, element <PredecessorIdentifier> can be used to identify the immediately preceding information package in the series and element <SuccessorIdentifier> can be used to identify the immediately succeeding information package. These elements have the following definitions

Tag Name	Element Description
PackageIdentifer	Required and contains the package identifier in its attributes. Element text is empty.
PredecessorIdentifier	Optional and contains the package identifier of the predecessor information package in its attributes. Element text is empty.
SuccessorIdentifier	Optional and contains the package identifier of the successor information package in its attributes. Element text is empty.

and all three elements use the same four attributes to identify the package:

Attribute	Attribute Description
site	Required and must be a standard NSE site identifier
identifier	Required and must be unique among information packages at the site
revision	Optional and must be an alphanumeric string
instance	Optional and must be an alphanumeric string

12.2.2 Elements <PackageDescription> and <PackageStatus>

Element <PackageDescription> is optional and contains a package description text string in its element text. This text string can contain any text except XML elements. Element <PackageStatus> is optional and can contain a phrase that describes the status of the information such as active, obsolete, released, or in process.

Element <PackageDescription> has this definition

Tag Name	Element Description
PackageDescription	Contains a description of the packaged information.
PackageStatus	Contains the status of the packaged information

These elements have no attributes.

12.2.3 Element <AlternateIdentifier>

Element <AlternateIdentifier> specifies an alternate identifier for the information package or the information in the information package. For example, if the information in the information package was obtained from another system, element <AlternateIdentifier> can be used to record the identifier of the information in that system.

Element <AlternateIdentifier> has this definition

Tag Name	Element Description
AlternateIdentifier	Specifies an alternate identifier for the information package or for the information in the information package in its element text.

and these attributes:

Attribute	Attribute Description
name	Required and must contain the name of the identifier
usedFor	Required and must be either package or information

The name attribute specifies the name of the identifier. The usedFor attribute can have one of two values: package or information. A value of package means that the identifier is for the whole package and a value of information means the identifier is for the information in the information package. For example, if the whole information package was stored in a separate system and had an identifier in that system separate from the identifier in the <PackageIdentifier> element, the <AlternateIdentifier> element can be used to specify that other system identifier.

12.2.4 Elements <CreatedTimestamp> and <ModifiedTimestamp>

The optional <CreatedTimestamp> and <ModifiedTimestamp> elements contain a timestamp that identifies the time the information package was created or updated. The timestamp is in the element text and should conform to the format specified in section x. These elements have this definition:

Tag Name	Element Description
CreatedTimestamp	Optional and contains the created timestamp in its element text.
ModifiedTimestamp	Optional and contains the modified timestamp in its element text.

These elements have no attributes.

12.3 ELEMENT <InformationMarking>

Element <InformationMarking> and its child elements <Classification> and <UnclassifiedControlled> contain the information marking required to protect the information in the information package. This element is designed assuming that most information stored in information packages will be information that is either classified or must be documented as unclassified. Accordingly, <Classification> is required both for classified and unclassified information. Element <Classification> for unclassified information documents that the data were determined to be unclassified by a specific reviewer, a review process, or came from a system not approved for classified information.

At least one <UnclassifiedControlled> element is required if the information is unclassified. An <UnclassifiedControlled> element provides the identification of and markings for one type of controlled information. When multiple types of controlled information are present in the information package, DOE marking rules require that markings for all types present must be used. For this reason, multiple <UnclassifiedControlled> elements may be required to protect the information in the information package. If the information is not controlled, an <UnclassifiedControlled> element documents this determination. Unclassified controlled information markings cannot be used when

classified information are present so an <UnclassifiedControlled> element must not be present when the information package contains classified information.

This element has the following definition:

Tag Name	Element Description
InformationMarking	Contains the information required to mark the document as required by DOE information security policies. Its element text has these elements in this order: one <Classification> element zero or more <UnclassifiedControlled> elements

and the following attribute:

Attribute	Attribute Description
default	Optional and must be either "yes" or "no"

Attribute default is used to document whether the information marking is a default marking assigned when the information package was created or is the result of an approved information review process such as review by a derivative classifier.

12.3.1 Element <Classification>

This element contains either the information marking required for classified information or documentation of a determination that the information in the information package is not classified. Its child elements identify the information classification level, category, and classifier and contain all required admonitory notices.

Element <Classification> has this definition:

Tag Name	Element Description
Classification	Contains the elements required for classified information or documentation of a determination that the information is not classified. these elements are in the element text in this order: one <Level> element zero or one <Category> element zero or more <Caveat> elements zero or more <SpecialControlMarking> elements zero or one <Admonishment> element zero or one <Title> element zero or one <OrganizationName> element zero or one <OrganizationAddress> element zero or one <DocumentDate> element zero or one <ClassifiedBy> element zero or one <DerivedFrom> element zero or one <DeclassifyOn> element zero or one <DateReviewed> element zero or more <AdditionalInformation> elements

Element <Classification> has no attributes.

12.3.1.1 Elements <Level> and <Category>

These elements specify the classification level and category and are defined as follows:

Tag Name	Element Description
Level	Contains the classification level in its element text. It must be one of these values: • Top Secret • Secret • Confidential • Unclassified
Category	Contains the classification category in its element text. It must be one of these values: • Restricted Data • Formerly Restricted Data • National Security Information

These elements have no attributes. Only one blank must separate the words in the level and category. The capitalization used is required because it is the capitalization used for these words in DOE manual 470.4-4A.

If the information in the information package is unclassified, the <Level> element must be present and contain Unclassified as its element text. The presence of Unclassified demonstrates to users that the information in the information package received a classification review when it was originated.

The classification category is required if the classification category is Restricted Data or Formerly Restricted Data. It is optional if the classification category is National Security Information. It must not be present if the classification level is Unclassified.

12.3.1.2 Elements <Caveat> and <SpecialControlMarking>

Elements <Caveat> and <SpecialControlMarking> identify special handling or dissemination requirements or assist in describing the type of information involved or who distributed or originated the information. Examples include Sigma level markings and the NOFORN caveat limiting distribution to foreign entities. See DOE manual DOE manual 470.4-4A for information on the contents required for these elements.

These elements are defined as follows:

Tag Name	Element Description
Caveat	Contain required caveats in its element text.
SpecialControlMarking	Contain required special control markings in its element text.

These elements have no attributes.

12.3.1.3 Element <Admonishment>

An admonishment statement is a statement that warns persons with access to the information about the consequences of releasing the information to unauthorized persons. An admonishment statement is required if the information package contains Restricted Data or Formerly Restricted Data. National Security Information and unclassified information do not have admonishment statements, so this element should not be present if Restricted Data or Formerly Restricted Data are not present in the information package.

This element has this definition:

Tag Name	Element Description
Admonishment	Contains the required admonishment statement in its element text.

This element has no attributes.

If the information package contains Restricted Data, the following text must be in the <Admonishment> element text:

RESTRICTED DATA This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended. Unauthorized disclosure is subject to Administrative and Criminal Sanctions.

If the information package contains Formerly Restricted Data but no Restricted Data, the following text must be in the <Admonishment> element text:

FORMERLY RESTRICTED DATA Unauthorized disclosure subject to Administrative and criminal sanctions. Handle as Restricted Data in Foreign Dissemination, Section 144.b, Atomic Energy Act, 1954.

12.3.1.4 Elements <Title>, <OrganizationName>, <OrganizationAddress> and <DocumentDate>

DOE manual 470.4-4A requires all documents to have a title or subject, origination organization name and address, and a date. The title or subject is placed in the <Title> element text and is marked as required by DOE manual 470.4-4A. The organization name is placed in the <OrganizationName> element text and the organization address is placed in the <OrganizationAddress> element. Both the name and address are entered as a text string. If the <CreatedTimestamp> or <ModifiedTimestamp> elements are not present in the <PackageIdentifiers> element, the <DocumentDate> element can be used to specify a document date. This date can be in any appropriate date format. Otherwise the date in the <CreatedTimestamp> or <ModifiedTimestamp> element serves as the document date.

These elements are defined as follows:

Tag Name	Element Description
Title	Contains the document title in its element text.
OrganizationName	Contains the name of the originating organization in its element text.
OrganizationAddress	Contains the address of the originating organization in its element text.
DocumentDate	Contains the date the document was originated in its element text.

These elements do not have attributes.

12.3.1.5 Elements <ClassifiedBy>, <DerivedFrom>, <DateReviewed> and <DeclassifyOn>

These elements represent the classifier markings required for classified documents by DOE manuals 470.4-4A and 475.1-1B. The classifier identification is placed in the <ClassifiedBy> element text, the source of the classification guidance is placed in the <DerivedFrom> element text, and for information packages that contain only National Security Information, declassification information is placed in the <DeclassifyOn> element text. The contents of the element text of these elements is specified by DOE manuals 470.4-4A and 475.1-1B.

This specification has element <DateReviewed> that specifies the date the document was reviewed. DOE manuals 470.4-4A and 475.1-1B assume that the document date is the date reviewed. However, information packages may not be formally reviewed until long after the packages are created. Furthermore, they may be changed after the formal review is performed without another classification review being performed. The <DateReviewed> element text contains the most recent date a formal classification review was performed on the information in the information package. A user can use this information to judge whether this classification review is valid for the information in the information package. This date can be in any standard date format.

These elements have this definition:

Tag Name	Element Description
ClassifiedBy	Contains the classifier identification in its element text. This identification conforms to the requirements of DOE manual 475.1-1B.
DerivedFrom	Contains the identification of the guidance used to determine the classification in its element text. This guidance identification conforms to the requirements of DOE manuals 470.4-4A and 475.1-1B.
DateReviewed	Contains the date the information was reviewed in its element text.
DeclassifyOn	Contains the declassification instructions in its element text. These instructions conform to the requirements of DOE manuals 470.4-4A and 475.1-1B.

The <ClassifiedBy> element has the attribute listed below and the other elements have no attributes.

Attribute	Attribute Description
type	Optional attribute that identifies the classifier type. It can be one of these values: • person – A person made the classification determination (default) • software – A computer program made the classification determination • default – The classification level and category were set at the highest level and category processed on the system

12.3.1.6 Element <AdditionalInformation>

The <AdditionalInformation> element is optional and can be used to provide additional information about the classification decision. The following are examples of additional information that can be stored using this element:

- Statement "Derivative Declassifier review required prior to declassification" required when the information package contains only NSI information.
- Sources used to make the classification determination when multiple sources are used
- Classification level and category matrix when the information package contains information in multiple classification categories
- Additional information about the classification process used when an automated process is used to make the classification determination

Each independent statement should be in a separate <AdditionalInformation> element. If additional information is not required, this element should not be present.

This element has this definition and has no attributes:

Tag Name	Element Description
AdditionalInformation	Contains additional information required to properly mark the information but not appropriate for any other element in its element text.

12.3.2 Element <UnclassifiedControlled>

Unclassified controlled information (UCI) is information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests. Twelve types of unclassified controlled information are currently defined and each type has its own marking requirements. An information package can contain more than one of these unclassified controlled information types. When it does, the DOE manuals require that the markings for each of the information types must be present.

The <UnclassifiedControlled> element is used to contain the markings for one type of unclassified controlled information. One<UnclassifiedControlled> element must be present in the <InformationMarking> element for each type of unclassified information present. This element represents one of these information types and contains child elements that contain required admonitory markings and other required information. The child elements of the <UnclassifiedControlled> element will depend on the type of information specified in its <Type> child element.

Element <UnclassifiedControlled> has the following definition.

Tag Name	Element Description
UnclassifiedControlled	Contains the elements required to properly mark unclassified controlled information or documentation of a determination that the information is not controlled. These elements are in the element text in this order: 1. one <Type> element 2. zero or more <Caveat> elements 3. zero or one <Admonishment> element 4. zero or one <ClassifiedBy> element 5. zero or one <NameOrganization> element 6. zero or one <Reviewer> element 7. zero or one <ReviewingOfficial> element 8. zero or one <DerivedFrom> element 9. zero or one <Guidance> element 10. zero or one <GuidanceUsed> element 11. zero or one <DateReviewed> element 12. zero or more <AdditionalInformation> elements

Element <UnclassifiedControlled> has no attributes.

Element <UnclassifiedControlled> child elements are described in alphabetical order below. Certain unclassified controlled information types require additional labeled information such as the identity of the person or entity that determined the unclassified controlled information type or the guidance used in that determination. The element tag names are designed to match as close as possible the labels used in the markings. In some cases elements with different tag names are used to represent basically the

same information. This specification assumes that the information marking for an unclassified controlled information type will use the element with the tag name that is the closest match to the label specified in the information type marking requirements.

12.3.2.1 Element <AdditionalInformation>

The <AdditionalInformation> element is optional and provides additional information about the marking. It can be used, for example to contain the foreign government markings when the information package contains Confidential/Foreign Government Information–Modified Handling information. Each independent set of information should be in a separate <AdditionalInformation> element. If additional information is not required, this element should not be present. This element has the same definition as the <AdditionalInformation> element used in classification markings.

12.3.2.2 Element <Admonishment>

An admonishment statement is a statement that warns persons with access to the information about the consequences of releasing the information to unauthorized persons. The admonishment statement is placed in the element text. The statement will depend on the type of controlled information present. This element has the same definition as the <Admonishment> element used in classification markings.

12.3.2.3 Element <Caveat>

Element <Caveat> identifies special handling or dissemination requirements or assists in describing the type of information involved or who distributed or originated the information. The contents of this element will depend on the type of controlled information present. This element has the same definition as the <Caveat> element used in classification markings.

12.3.2.4 Elements <ClassifiedBy> and <DerivedFrom>

Elements <ClassifiedBy> and <DerivedFrom> are used for information packages containing Confidential/Foreign Government Information–Modified Handling information. These elements are the same as the elements used in classifier marking and are described above.

12.3.2.5 Element <DateReviewed>

Element <DateReviewed> contains the date the information type determination was made. This date does not have to conform to the date and time formats recommended in this specification. It has the same definition as the element used in the classifier marking.

12.3.2.6 Element <Guidance> and <GuidanceUsed>

The guidance used to make a determination is entered in the element text of the <Guidance> and <GuidanceUsed> elements. The content of these elements is specified by the requirements of the information type. These elements are defined below and have no attributes:

Tag Name	Element Description
Guidance	Contains the guidance used to determine the unclassified controlled information type.
GuidanceUsed	Contains the guidance used to determine the unclassified controlled information type.

12.3.2.7 Elements <NameOrganization>, <ReviewingOfficial>, and <Reviewer>

Elements <ReviewingOfficial>, <NameOrganization>, and <Reviewer> contain the identity of the person or entity that determined the unclassified controlled information type. These elements are defined below and have no attributes

Tag Name	Element Description
NameOrganization	Contains the name and organization of the person or entity that determined the unclassified controlled information type.
ReviewingOfficial	Contains the identity of the person or entity that determined the unclassified controlled information type.
Reviewer	Contains the identity of the person or entity that determined the unclassified controlled information type.

12.3.3 Element <Type>

The <Type> element contains the name of the controlled information type in its element text. This element is defined as follows and has no attributes:

Tag Name	Element Description
Type	Contains the unclassified controlled information type or Not Controlled if the information is not controlled.

The current list of information types at Y-12 is:

- Unclassified Controlled Nuclear Information
- Export Controlled Information
- Naval Nuclear Propulsion Information
- Safeguards Information
- Sensitive Nuclear Technology
- Official Use Only
- Applied Technology
- Cooperative Research and Development Agreement
- Confidential/Foreign Government Information-Modified Handling
- Privacy Act information
- Proprietary Information
- Contractor Information

The information type should be spelled and capitalized exactly as shown in the list above. Only one blank must separate the words in the type name. If a new type of controlled information is defined, this type should be added to the list and capitalized as shown above.

12.4 ELEMENT <AccessControl>

Element <AccessControl> provides an information management system with the information required to determine whether the system should allow or deny a user or application access to the information in the information package. An information management system is expected to get the information attributes associated with the information package directly from the information package or from a separate set of metadata created from the information attributes when the information package was stored. The information management system is expected to compare the information attributes obtained from the information package with access control rules that determine whether the user or application has access. If the access control rules allow access, access is granted; otherwise it is denied.

The <AccessControl> element is defined as follows:

Tag Name	Element Description
AccessControl	Contains information access control attributes contain in zero or more <InfoAttribute> elements.

Element <InfoAttribute> contains an information attribute organized as a name-value pair. The name is specified by an optional name attribute and the value is specified in the element text. Any number of <InfoAttribute> elements can be included in the <AccessControl> element when the package is created and new elements can be added or existing elements modified or deleted as required over time.

The <InfoAttribute> element is defined as follows:

Tag Name	Element Description
<InfoAttribute>	Contains an optional name attribute that specifies the element name and a required value in the element text.

The name attribute is defined as follows:

Attribute	Attribute Description
name	Optional and contains the information attribute name.

12.5 ELEMENT <SearchTerms>

This element contains a set of search terms that can be used to locate the information package when it is stored in an information repository. Each search term contains a search term and optional attributes that specify the name of the search term and the units of measure used for the search term. All search terms are children of the <SearchTerms> element.

The <SearchTerms> element has the following definition:

Tag Name	Element Description
<SearchTerms>	Contains zero or more search term <SearchTerm> elements.

<SearchTerms> has no attributes.

12.5.1 10.5.1 Element <SearchTerm>

This element defines a single search term value and has this definition:

Tag Name	Description
<SearchTerm>	Contains a search term in its element text.

Element <SearchTerm> has two optional attributes that specify a name for the search term and the units of measure for the search term value:

Attribute	Attribute Description
name	Optional attribute that specifies a search term name.
units	Optional attribute that specifies units of measure for the search term value.

12.5.2 Example

The following example shows what a set of search terms might look like:

```
<SearchTerms>
  <SearchTerm name=”inspection type”>
 weight inspection
  </SearchTerm>
  <SearchTerm name=”weight”units=”kg”>
  1.000
  </SearchTerm>
</SearchTerms>
```

12.6 ELEMENT <History>

This element documents the history of the information package and its information. It contains a series of <Event> elements each of which describes one event in the history of the information package or its information. If this history starts before the information package is created, the <Event> elements that record this history may be added when the package is created. Every time the package is revised, an <Event> element can be added to record information about the revision.

The <History> element has the following definition:

Tag Name	Element Description
History	Contains zero or more event <Event> elements in its element text.

<History> has no attributes and its element text consists only of zero or more <Event> elements. The <Event> elements should be in chronological order with the oldest immediately following the <History> element. An <Event> element should not be removed from the <History> element.

12.6.1 Element <Event>

This element contains information about a single event. This event can be data creation, data revision, package creation, package revision, or any other event that impacts the information or information package. Each <Event> element should describe one event and the events should be in chronological order with the oldest immediately following the <History> element. This element has this definition:

Tag Name	Element Description
Event	Contains an event description in its element text.

The attributes on the <Event> element describe the source of the event information. Event information includes the identity of the person or program that added the event, the time the event was added, and whether the event changed the information in the <PackageInfo> element. This table lists the attributes used:

Attribute	Attribute Description
name	Person or program name
employeeId	Employee identifier such as employee number (if known)
site	Site identifier
time	Date and time of the event in standard format.
packageInfoChanged	Set to “yes” if the signed contents were changed, empty or “no” otherwise

If the source of the event is a program, the name attribute contains the program name and version and the employee identifier is absent. If the source of the event is a person, the name attribute contains the person’s name and the employee identifier contains the person’s employee number, badge number, or similar value. In both cases the site specifies the site and the time specifies the date and time of the event.

The event description is entered in <Event> element text. This description can be standard text or any text desired by the event source.

12.7 ELEMENT <Notes>

This element records notes about the information package and the information contained in the information package.

Examples of appropriate notes include:

- Source of the information in the information package

- Quality of the information in the information package
- Reason the information package was modified

Element <Notes> has the following definition:

Tag Name	Element Description
Notes	Contains zero or more note <Note> elements in its element text.

Element <Notes> has no attributes. <Note> elements should be in chronological order with the oldest immediately following <Notes>.

12.7.1 Element <Note>

This element contains a single note. A note should be restricted to one topic. Multiple topics should be in separate <Note> elements with one topic per element. <Note> has this definition:

Tag Name	Element Description
Note	Contains one note in its element text.

Attributes of <Note> describe the source of the note. Source information includes the identity of the person or program that added the note and the time the note was added. This table lists the attributes used:

Attribute	Description
name	Person or program name
employeeId	Employee identifier (if known)
site	Site identifier
time	Date and time the information package was updated

If the source of the note is a program, the name attribute contains the program name and version and the employee identifier is absent. If the source of the note is a person, the name attribute contains the person's name and the employee identifier contains the person's employee number, badge number, or similar value. In both cases the site specifies the site and the time specifies the date and time the note was added.

The note is entered in <Note> element text. This description can be standard text or any text desired by the note source.

12.8 ELEMENT <References>

Element <References> contains <Reference> elements that identify related information packages. Each <Reference> element specifies another information package by its site and identifier. If the referenced information package has revision and/or instance values, the reference attribute may use them in the reference. The meaning of the reference if the referenced information package has revision and/or instance values and the reference element does not use them is outside the scope of this specification.

Element text contains a description of the reference. The format and contents of this description are outside the scope of this specification.

Element <References> has this definition:

Tag Name	Element Description
References	Contains references to related information packages as zero or more <Reference> elements

This element has no attributes.

12.8.1 Element <Reference>

Element <Reference> identifies the related information package and has this definition

Tag Name	Element Description
Reference	Optional and identifies the reference information package in its attributes. Element text describes the relationship.

It uses the same attributes as <PackageIdentifier> to identify the related package:

Attribute	Attribute Description
site	Required and must be a standard NSE site identifier
identifier	Required and must be unique among information packages at the site
revision	Optional and must be an alphanumeric string
instance	Optional and must be an alphanumeric string

The <Reference> elements can be in any order. If an order is present, its meaning is outside the scope of this specification.

12.9 ELEMENT <PackageInfo>

This element contains the information the package was created to contain. There are no restrictions on the form of this information. This element has this signature:

Tag Name	Element Description
PackageInfo	Contains the information package information and the <Signature> element that protects this information in its elemen text. The format and structure of the information is not specified.

If PackageInfo and all of its contents must be protected by an XML signature, this element must have the following attribute:

Attribute	Attribute Description
id	Optional and must be SignedContents

12.9.1 Element <Signature>

This element contains information about the XML signature used to sign the information in <PackageInfo>. This information includes the identity of the protected information, the method used to create a message digest of the protected information, the method used to sign the protected information message digest, the digital signature, and the certificate that holds the public key that corresponds to the private key used to sign the message digest.

This information allows a user to determine whether the information in <PackageInfo> has been altered. The user can repeat the process used to generate the digital hash from the current information. The user uses the public key in the certificate to decrypt the encrypted digital hash. If the two hash values are the same, the information has not been altered.

13. INFORMATION PACKAGE CREATION, REVISION, AND USE

Information packages can be used to store information as it is collected and identified and information already in repositories. Information packages should be stored in an information management system that will provide configuration control for the packages and the tools required by users to locate and extract them from the system. When information marking, access control, or search term requirements change, information packages can be revised to meet the new requirements without affecting the information stored in them. At any time they can be extracted from the product information system and used in weapon surveillance or process improvement activities.

13.1 INFORMATION MANAGEMENT SYSTEMS

Information packages should be stored in and managed using an information management system such as a product information management system. These systems provide tools that allow systems that create information packages to store the packages and users to locate and extract the packages they need. Information management systems also provide configuration management tools used to manage information package revisions. These systems are backed up to prevent information package loss.

13.2 INFORMATION PACKAGE CREATION

Most information packages containing product information will be created by software from information stored in existing repositories and from information collected during production or inspection activities. The resulting information packages will be stored in a product information management system. The software that creates the package from information in an existing repository will likely be associated with the existing repository. The software that creates an information package for information collected during production or inspection activities may be associated with the activity or the product information management system.

The software that creates the information package must have access to related information so it can store the context required to understand the information in the information package and add to it the correct information marking, access control, and search terms. This related information may be obtained from a product information management or enterprise resource planning system. To create an information package from new or existing data, the software may use this process:

- Store the information in the information package.
- Add the context required to understand and use the information to the information package. This context may include product information, part serial number, material, machine number, timestamp, etc.
- Use product information to generate the information marking and access control required.
- Use stored information, its context, and associated product information to create the search terms.
- Create the XML signature for the information that must be protected.
- Store the information package in the product information management system.

If a product information management system will be used to store the information, it may follow this process:

- Store the information package in the product structure according to the information in the information package.
- Use the information in the <AccessControl> element to set the parameters required to limit access to the information and functions that act on the information package to authorized users.
- Use the information in the <SearchTerms> element to set the values of attributes searched by the product information management system search tools.

At the end of this process, the information package is stored in the information management system in the appropriate location with search attributes required to independently locate the information package

13.3 INFORMATION PACKAGE REVISIONS

An information package can be revised when necessary to change the access control, information marking, or search terms, to add a note or history event, or to change packaged information. A package is revised by copying the old package to a new package and assigning it a unique identifier with optional revision and instance. The status of the old package can be set to obsolete and the new package identifier (and revision and instance if used) stored in the old package <SuccessorIdentifier> element. The unique identifier (with revision and instance if used) of the old package can be stored in the new package <PredecessorIdentifier> element. The reason for the revision can be included as an event in the package history. If the information in <PackageInfo> is changed, the history <Event> element packageInfoChanged attribute can be used to record the change.

Information packages are designed to allow the information marking, access control, search term, and other metadata or package information to change while protecting the packaged information that must be protected. An XML signature protects information in <PackageInfo> or in one or more child elements of <PackageInfo>. At any time a new XML signature can be calculated for the protected information. If the calculated signature matches the signature in the package, the signed information has not changed since the original signature was calculated. In this way a user of this information knows that the information is original even though the package may have been revised several times. If the signed information was changed in the revision, a new XML signature must be calculated and the signature information stored in the <Signature> element. The information in the public key certificate can be used to identify when a signature was calculated.

13.4 INFORMATION PACKAGE USE

A user can get the information required to perform an analysis from information packages by following this process:

- Locate the information packages in the information management system that contain the information needed for the analysis. The search may be a general search that returns more information packages than those required for the analysis.
- Extract the information packages from the information management system.

- Store the extracted information packages in an XML database.
- Use XML database tools to identify the set of information packages in the database that contain the information required for the analysis.
- Use XML database tools to create a comma separated value (CSV) file containing the information required for the analysis from the identified set of information packages.
- Use an analysis tool such as Microsoft Excel to read the CSV file containing the data.
- Use analysis tool functions to analyze the data.

13.5 SEARCH AND RETRIEVAL

A user can locate information packages stored in an information management system by following the information structure to the package or by searching for information packages with specified search attribute values. Once located, the user can retrieve the information packages from the information management system. A user following the information structure can be expected to find and retrieve one information package at a time. A user searching for information packages using search attributes will find and retrieve a set of information packages.

A user that uses information structure to identify information packages will get exactly the set of packages needed but will spend more time getting those packages. A user that searches for information packages can be expected to get packages that do not contain relevant information but will get them faster. The information packages retrieved and the methods used to retrieve them should be documented to ensure that they can be retrieved again.

13.6 LOCAL ANALYSIS

Once the set of information packages that contain required information are retrieved, they must be loaded into an XML database that belongs to the user or the user's organization. The XML database will allow the user to use the full power of XML tools to search for and extract information from the information packages. Using XML tools, a user can search for information packages with specific information values and save these packages as a subset.

The user can then use other XML tools to extract values from these information packages and save them in a comma separated value file. This file would contain one record for each information package with its fields containing the same values from each package. This file can be read and parsed by Microsoft Excel and by many other data analysis packages. When Excel reads the file, it stores each record in a row and each record value in a column with text stored as text and numbers stored as numeric values. The result is a column of values in Excel that can be manipulated and processed using Excel tools. The CSV file can easily be transformed into formats required by other tools. The analyst performs the required analyses and reports the results.

13.7 USAGE SCENARIO

This unclassified usage scenario shows how information packages can be used as a source of product and process information in surveillance and process improvement activities. This scenario is fictitious and

is completely unrelated to any work now or previously performed at Y-12. The scenario assumes that a part is assembled into a product assembly. Before the part is placed in the product assembly, it is weighed and its weight recorded in a product information package. This product information package is stored in a product information system for later analysis.

The part is made of steel, weighs approximately 1 kg, and is identified by a serial number. The part is described by drawing D010 and this drawing specifies the steel alloy to be used to make the part. The first set of parts produced used material Steel1 as specified on drawing D010-00. During the production run, drawing D010-01 was released that specified the use of material Steel2. Parts built using steel alloy Steel2 are 10 g heavier than parts built using steel alloy Steel1.

The weigh station is in facility F001 and has two scales identified as scales S001 and S002. Scale S001 measures weights in grams and scale S002 measures weights in kilograms. Each scale is attached to a separate data acquisition system that can get the weight from the attached scale, create a part weight information package containing the weight, and store that part weight information package in the plant product information management system. Both scales are used to weigh several different types of parts and operators are expected to wait for and use the next available scale to weigh a part.

A manufacturing execution system is used to manage the production process. The MES routing used to create part D010 is called D010Route and the operation in which the part is weighed is assigned operation code WT01.

The scales are operated by two operators: A. B. Jones, employee number E101, and C. D. Smith, employee number E202. Both employees have the same training and follow this procedure to weigh parts:

1. Wait for one of the scales to become available.
2. Prepare the scale and data acquisition system to weigh the part.
3. Enter the operator employee number and part serial number in the data acquisition system.
4. Place part on scale.
5. Instruct the data acquisition system to collect the weight.
6. Data acquisition system gets the weight from the scale, creates an information package to store it, and sends that information package to the product information management system.

Because of slight differences in how they execute this procedure, weights measured by C. D. Smith are 5 grams heaver than weights measured by A. B. Jones.

This production run produced 20 parts to be placed in the product assembly. The part material changed halfway through the production run. A. B. Jones and C. D. Smith each weighed half of the parts and they used the next available scale to weigh each part. The following data were collected and stored in information packages:

Drawing	Material	Serial No	Emp No	Scale	Weight
D010-00	Steel1	8001	E101	S001	991. g
D010-00	Steel1	8002	E101	S002	.992 kg
D010-00	Steel1	8003	E202	S001	998. g
D010-00	Steel1	8004	E202	S002	.999 kg

Drawing	Material	Serial No	Emp No	Scale	Weight
D010-00	Steel1	8005	E101	S001	995. g
D010-00	Steel1	8006	E101	S002	.996 kg
D010-00	Steel1	8007	E202	S001	1002. g
D010-00	Steel1	8008	E202	S002	1.003 kg
D010-00	Steel1	8009	E101	S001	999. g
D010-00	Steel1	8010	E101	S002	1.000 kg
D010-01	Steel2	8011	E202	S001	1006. g
D010-01	Steel2	8012	E202	S002	1.007 kg
D010-01	Steel2	8013	E101	S001	1003. g
D010-01	Steel2	8014	E101	S002	1.004 kg
D010-01	Steel2	8015	E202	S001	1010. g
D010-01	Steel2	8016	E202	S002	1.011 kg
D010-01	Steel2	8017	E101	S001	1007. g
D010-01	Steel2	8018	E101	S002	1.008 kg
D010-01	Steel2	8019	E202	S001	1014. g
D010-01	Steel2	8020	E202	S002	1.015 kg

When creating the information package, each data acquisition system also added the part weight in kilograms to the package. This weight allows searchers to search for part weight information packages using weight in kilograms to filter the selection. The signed information package used to store the information collected for part 8001 is shown in Appendix A.

After the production run ended, a process analyst was directed to examine the collected data to determine whether weight anomalies existed and, if so, the cause of these anomalies. The analyst extracted the product information packages that contained the data in the table above and stored them in a Berkeley DB XML database [XML DB] named PartWeights.dbxml. This database system is provided and supported by Oracle Corporation and is free for noncommercial use. The analyst could have used any other database that supports XML queries such as Oracle 11g or Microsoft SQLServer. The analyst used this script to create a comma-separated value file of the data in the above table:

```
open PartWeights.dbxml
setNamespace ip urn:x-y12:InfoPackage
query '
    for $d in collection("PartWeights.dbxml")
    return concat(
        $d/ip:InfoPackage/ip:PackageInfo/ProductInfo/Product/DrawingNumber/string(),
        ",",
        $d/ip:InfoPackage/ip:SearchTerms/ip:SearchTerm[@name="material"]/string(),
        ",",
        $d/ip:InfoPackage/ip:PackageInfo/ProductInfo/Product/SerialNumber/string(),
        ",",
        $d/ip:InfoPackage/ip:PackageInfo/ProductInfo/Operators/Operator/
        @employeeId/string(),
```

```
        ",",
        $d/ip:InfoPackage/ip:PackageInfo/ProductInfo/Data/DataValue
        [Name="machine identifier"]/Value/string(),
        ",",
        $d/ip:InfoPackage/ip:PackageInfo/ProductInfo/Data/DataValue
        [Name="weight"]/Value/string(),
        ",",
        $d/ip:InfoPackage/ip:PackageInfo/ProductInfo/Data/DataValue
        [Name="weight"]/Value/@units/string(),
        ",",
        $d/ip:InfoPackage/ip:SearchTerms/ip:SearchTerm
        [@name="weight kg"]/string())'
print PartWeights.csv
```

This query also added the part weight in kilograms to the file. The query and the following print instruction created this CSV file:

```
D010-00,Steel1,8001,E101,S001,991.,g,.991
D010-00,Steel1,8002,E101,S002,.992,kg,.992
D010-00,Steel1,8003,E202,S001,998.,g,.998
D010-00,Steel1,8004,E202,S002,.999,kg,.999
D010-00,Steel1,8005,E101,S001,995.,g,.995
D010-00,Steel1,8006,E101,S002,.996,kg,.996
D010-00,Steel1,8007,E202,S001,1002.,g,1.002
D010-00,Steel1,8008,E202,S002,1.003,kg,1.003
D010-00,Steel1,8009,E101,S001,999.,g,.999
D010-00,Steel1,8010,E101,S002,1.000,kg,1.000
D010-01,Steel2,8011,E202,S001,1006.,g,1.006
D010-01,Steel2,8012,E202,S002,1.007,kg,1.007
D010-01,Steel2,8013,E101,S001,1003.,g,1.003
D010-01,Steel2,8014,E101,S002,1.004,kg,1.004
D010-01,Steel2,8015,E202,S001,1010.,g,1.010
D010-01,Steel2,8016,E202,S002,1.011,kg,1.011
D010-01,Steel2,8017,E101,S001,1007.,g,1.007
D010-01,Steel2,8018,E101,S002,1.008,kg,1.008
D010-01,Steel2,8019,E202,S001,1014.,g,1.014
D010-01,Steel2,8020,E202,S002,1.015,kg,1.015
```

The analyst used Microsoft Excel to read this CSV file. Excel stored each of the comma-separated values in a separate column with text values stored as text and numeric values stored as their Excel numeric equivalents.

The analyst used Excel tools to calculate these average part weights for each material:

Steel1 average part weight	0.9975
Steel2 average part weight	1.0085
Difference	0.011

The analyst then measured the differences in the weights produced by the two operators:

E101 average part weight	0.9995
E202 average part weight	1.0065
Difference	0.007

Operator Smith weighed more Steel2 parts than operator Jones, and this may have affected the results. When the weights are separated by material type, the weight differences are:

E202 Steel1 weight difference	0.005
E202 Steel2 weight difference	0.005

This analysis shows the perceived anomaly is real and enables management to take action to reduce it such as by modifying or clarifying procedures.

The analyses that can be performed using the data in the CSV file are limited only by the capabilities of Excel and its user. The script above can easily be modified to get additional information which would allow an analyst to perform other studies.

ACRONYMS

AT	Applied Technology
C/FGI-MOD	Confidential/Foreign Government Information—Modified Handling
CRADA	Cooperative Research and Development Agreement
CSV	Comma-Separated Value
DOE	Department of Energy
DOE/NE	DOE Office of Nuclear Energy, Science, and Technology
DOM	Document Object Model
DSS	Digital Signature Standard
DSSSL	Document Style Semantics and Specification Language
ECI	Export Controlled Information
FIPS	Federal Information Processing Standard
FRD	Formerly Restricted Data
HTML	Hypertext Markup Language
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NSI	National Security Information
NNP	Naval Nuclear Propulsion
NNPA	Nuclear Nonproliferation Act
NNSA	National Nuclear Security Administration
NSE	Nuclear Security Enterprise
OUO	Official Use Only
PRIDE	Product Realization Integrated Digital Enterprise
RD	Restricted Data
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SI	Safeguards Information International System of Weights and Measures
SNT	Sensitive Nuclear Technology
UCI	Unclassified Controlled Information
UCNI	Unclassified Controlled Nuclear Information
W3C	World Wide Web Consortium
XML	Extensible Markup Language
XPath	XML Path Language
XQuery	XML Query Language
XSLT	XSL Transformations

XSL-FO	XSL Formatting Objects

REFERENCES

[C14N10]
J. Boyer, ed. *Canonical XML Version 1.0.* W3C Recommendation, World Wide Web Consortium (W3C), http://www.w3.org/TR/xml-c14n15 March 2001.

[C14N11]
Canonical XML Version 1.1. W3C Recommendation, World Wide Web Consortium (W3C), http://www.w3.org/TR/xml-c14n11/2 May 2008.

[DOE M 470.4-4A]
Information Security Manual. DOE manual 470.4-4AU.S. Department of Energy, January 16, 2009.

[DOE M 471.1-1]
Identification and Protection of Unclassified Controlled Nuclear Information Manual. DOE manual 471.1-1U.S. Department of Energy, October 23, 2001.

[DOE M 471.3-1]
Manual for Identifying and Protecting Official Use Only Information. DOE manual 471.3-1U.S. Department of Energy, April 9, 2003.

[DOE M 475.1-1B]
Manual for Identifying Classified Information. DOE manual 475.1-1BU.S. Department of Energy, August 28, 200.

[FIPS 180-3]
Secure Hash Standard (SHS). Federal Information Processing Standards Publication 180-3National Institute of Standards and Technology, October 2008.

[FIPS 186-3]
Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-3National Institute of Standards and Technology, June 2009.

[ISO 8601]
Data elements and interchange formats – Information interchange – Representation of dates and times. ISO 8601:2004International Organization for Standardization, 2004.

[NIST 44]
Specifications, Tolerances, and Other Technical Requirements for Weighing and Measuring Devices. NIST Handbook 44, 2009 editionNational Institute of Standards and Technology, 2009.

[PKCS1]
B. Kaliski, J. Staddon. *PKCS #1: RSA Cryptography Specifications Version 2.0.* RFC 2437Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc2437.txtOctober 1998.

[RFC 822]
David H. Crocker. *Standard For The Format Of ARPA Internet Text Messages.* The Internet Society, August 13, 1982.

[RFC 2141]
R. Moats. *URN Syntax.* The Internet Society, May 1997.

[RFC 3406]
L. Daigle, D. W. van Gulik, R. Iannella, P. Faltstrom. *Uniform Resource Names (URN) Namespace Definition Mechanisms.* The Internet Society, October 2002.

[RFC 4648]
The Base16, Base32, and Base64 Data Encodings. RFC 4648Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc4648.txtOctober 2006.

[SI]
Le Système international d'unités—The International System of Units (SI). International Bureau of Weights and Measures (BIPM), Sèvres, France, http://www.bipm.org/utils/common/pdf/si_brochure_8_en.pdf2006.

[W3C Datetime]
. *Date and Time Formats.* W3C Note, World Wide Web Consortium (W3C), http://www.w3.org/TR/NOTE-datetimeaccessed on August 27, 2009, http://www.w3.org/Consortium/Legal/2002/copyright-documents-20021231.

[XML 2006]
Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Francois Yergeau, and Eve Maler, eds. *Extensible Markup Language (XML) 1.0 (Fourth Edition).* W3C Recommendation, World Wide Web Consortium (W3C), http://www.w3.org/TR/REC-xml/16 August 2706.

[XML DB]
Oracle Berkeley DB XML. Oracle Corporation, http://www.oracle.com/technology/products/berkeley-db/xml/index.htmlRetrieved on September 23, 2009.

[XMLDSIG 2002]
Eastlake, Donald, et. al., eds. *XML-Signature Syntax and Processing.* W3C Recommendation, World Wide Web Consortium (W3C), http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/February 2002.

[XMLDSIG 2008]
Eastlake, Donald, et. al., eds. *XML-Signature Syntax and Processing (Second Edition).* W3C Recommendation, World Wide Web Consortium (W3C), http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/ 10 June 2008.

[XMLNamespaces]
Tim Bray, Dave Hollander, Andrew Layman, and Richard Tobin, eds. *Namespaces in XML 1.0 (Second Edition).* W3C Recommendation, World Wide Web Consortium (W3C), http://www.w3.org/TR/REC-xml-names/.

[Y19-206]
Manual for Unclassified Controlled Information. Management Requirements, Number Y19-206BWXT Y-12, L.L.C., September 28, 2006.

APPENDIX A

INFORMATION PACKAGE EXAMPLE

This signed information package was created for the information package usage scenario in section 13 and contains the part 8001 weight collected by A. B. Jones using scale S001 . The package includes a package identifier, information marking, access control, search terms, package history, and the context for the weight. Elements defined by this specification use the information package namespace and `ip:` prefix and XML signature elements use the XML Signature namespace and `ds:` prefix.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ip:InfoPackage SYSTEM "PartInfoPackage.dtd">
<ip:InfoPackage version="1.0" xmlns:ip="urn:x-y12:InfoPackage">
  <ip:PackageIdentifiers>
    <ip:PackageIdentifier identifier="D010-00-8001-WT" instance="1" site="Y-12"/>
    <ip:PackageDescription>
      Information package specification demonstration information package
    </ip:PackageDescription>
    <ip:CreatedTimestamp>2009-09-01T01:01:00.000-04:00</ip:CreatedTimestamp>
  </ip:PackageIdentifiers>
  <ip:InformationMarking default="no">
    <ip:Classification>
      <ip:Level>Unclassified</ip:Level>
    </ip:Classification>
    <ip:UnclassifiedControlled>
      <ip:Type>Not Controlled</ip:Type>
      <ip:Reviewer>Matthew Kelleher, Y-12 IT DC/RO</ip:Reviewer>
    </ip:UnclassifiedControlled>
  </ip:InformationMarking>
  <ip:AccessControl>
    <ip:InfoAttribute name="drawing">D010</ip:InfoAttribute>
    <ip:InfoAttribute name="material">Steel1</ip:InfoAttribute>
  </ip:AccessControl>
  <ip:SearchTerms>
    <ip:SearchTerm name="drawing">D010-00</ip:SearchTerm>
    <ip:SearchTerm name="material">Steel1</ip:SearchTerm>
    <ip:SearchTerm name="serial number">8001</ip:SearchTerm>
    <ip:SearchTerm name="information type">inspection</ip:SearchTerm>
    <ip:SearchTerm name="inspection type">weight</ip:SearchTerm>
    <ip:SearchTerm name="weight kg">.991</ip:SearchTerm>
  </ip:SearchTerms>
  <ip:History>
    <ip:Event employeeId="E101" name="A. B. Jones" packageInfoChanged="yes" site="Y-12"
      time="2009-09-01T01:01:00.000-04:00"> Package created. </ip:Event>
  </ip:History>
  <ip:Notes/>
  <ip:References/>
  <ip:PackageInfo>
    <ProductInfo id="SignedContents">
```

```
    <Contents>
      <InformationType>weight measurement</InformationType>
      <Description>Part weight</Description>
    </Contents>
    <Product>
      <DrawingNumber>D010-00</DrawingNumber>
      <SerialNumber>8001</SerialNumber>
    </Product>
    <Process>
      <Facility>F001</Facility>
      <Route>D010Route</Route>
      <Operation>WT01</Operation>
    </Process>
    <Data>
      <DataValue>
        <Name>weight</Name>
        <Value units="g">991.</Value>
      </DataValue>
      <DataValue>
        <Name>machine identifier</Name>
        <Value>S001</Value>
      </DataValue>
    </Data>
    <Operators>
      <Operator employeeId="E101" name="A. B. Jones" site="Y-12"
        time="2009-09-01T01:01:00.000-04:00"/>
    </Operators>
  </ProductInfo>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
      <ds:Reference URI="#SignedContents">
        <ds:Transforms>
          <ds:Transform
            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>ige0OMEXEd05upAAFdzZXL+b39A=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      QnIr3l8+6/2sT5/blIEQZ2g6mb8VhH5Cd8JJW9Hb+QpSO3p5GyImLA==
    </ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509SubjectName>CN=infopackage.y12.gov,OU=Information Technology,O=Y-12
          Complex,L=Oak Ridge,ST=Tennessee,C=US</ds:X509SubjectName>
        <ds:X509Certificate>
          MIIDTzCCAw2gAwIBAgIESrErxjALBgcqhkjOOAQDBQAwgYoxCzAJBgNVBAYTAlVTMRIwEAYDVQQI
```

```
            EwlUZW5uZXNzZWUxEjAQBgNVBAcTCU9hayBSaWRnZTEUMBIGA1UEChMLWS0xMiBDb21wZXgxHzAd
            BgNVBAsTFkluZm9ybWF0aW9uIFRlY2hub2xvZ3kxHDAaBgNVBAMTE2luZm9wYWNrYWdlLnkxMi5n
            b3YwHhcNMDkwOTE2MTgxNzQyWhcNMTEwOTA2MTgxNzQyWjCBijELMAkGA1UEBhMCVVMxEjAQBgNV
            BAgTCVRlbm5lc3NlZTESMBAGA1UEBxMJT2FrIFJpZGdlMRQwEgYDVQQKEwtZLTEyIENvbXBleDEf
            MB0GA1UECxMWSW5mb3JtYXRpb24gVGVjaG5vbG9neTEcMBoGA1UEAxMTaW5mb3BhY2thZ2UueTEy
            LmdvdjCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQD9f1OBHXUSKVLfSpwu7OTn9hG3UjzvRADDHj+A
            tlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSfn+gEexAiwk+7qdf+t8Yb
            +DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgBxwIVAJdgUI8VIwvMspK5
            gqLrhAvwWBz1AoGBAPfhoIXWmz3ey7yrXDa4V7l5lK+7+jrqgvlXTAs9B4JnUVlXjrrUWU/mcQcQ
            gYC0SRZxI+hMKBYTt88JMozIpuE8FnqLVHyNKOCjrh4rs6Z1kW6jfwv6ITVi8ftiegEkO8yk8b6o
            UZCJqIPf4VrlnwaSi2ZegHtVJWQBTDv+z0kqA4GEAAKBgCm9ncRDbugOvR9LGRMXnFCu2u5BAAJJ
            f3iLB108E3B6ymsa1zcwq7uemNvgZnzFNm4UfgcMRuhnUenyJIwCoSu8a91N0vQXSuewS7t0Z/7M
            Ge9vwH494bfvAJ8MBIe5qlMLKelTYr5fnGJPjsWPQ3yFVLqo/SHqQNqs+qX8wBc2MAsGByqGSM44
            BAMFAAMvADAsAhQbnAxxEbo67W3tl+Kq/qzcM3yfEQIUXP7XGNZ9D6CxnjDntlBsMfkt4/Q=
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
   /ip:PackageInfo>
</ip:InfoPackage>
```

APPENDIX B

UNCLASSIFIED CONTROLLED INFORMATION MARKING REQUIREMENTS

Section 5 specifies the marking requirements for Unclassified Controlled Nuclear Information (UCNI) and for Official Use Only (OUO) information and defines the elements used to mark other types of unclassified controlled information. This section specifies the marking requirements for other types of unclassified controlled information used at the Y-12 National Security Complex. The information in this section was obtained from Y-12 manual Y19-206 *Manual for Unclassified Controlled Information* [Y19-206].

In every case an admonitory marking must be added to the document to inform users that the specified type of information is present in the information package This admonitory marking has text in capital letters and may have text in sentence case. This capitalization must be used in the `<Admonishment>` element text.

Additional elements must be added in certain cases to identify the person or entity that made the unclassified controlled information type determination. These elements are specified in the section that requires them.

B.1 EXPORT CONTROLLED INFORMATION

Export Controlled Information is certain scientific and technical information products containing technical data as defined in and controlled by the International Traffic in Arms Regulations, Export Administration Regulations, Nuclear Nonproliferation Act of 1978 (NNPA), and the Atomic Energy Act of 1954, as amended.

If the information package contains Export Controlled information, an `<UnclassifiedControlled>` element must be present with a `<Type>` element containing as its element text with single blank character separating all words:

`Export Controlled Information`

The following text must appear in the `<Admonishment>` element text:

EXPORT CONTROLLED INFORMATION Contains technical data whose export is restricted by statute. Violations may result in administrative, civil, or criminal penalties. Limit dissemination to U.S. Department of Energy and major U.S. DOE contractors. The cognizant program manager must approve other dissemination. This notice shall not be separated from the attached document.

The name of the reviewer is placed in the `<Reviewer>` element text and the date the review was performed is placed in the `<DateReviewed>` element text.

B.2 NAVAL NUCLEAR PROPULSION INFORMATION

Naval Nuclear Propulsion Information is information about the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, or repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities.

If the information package contains Naval Nuclear Propulsion information, an `<UnclassifiedControlled>` element must be present with a `<Type>` element containing as its element text with single blank character separating all words:

`Naval Nuclear Propulsion Information`

The following text must appear in the `<Admonishment>` element text:

NOFORN. This document is subject to special export controls and each transmittal to foreign governments or foreign nationals must be made only with the prior approval of the NavSea.

B.3 SENSITIVE NUCLEAR TECHNOLOGY

Sensitive Nuclear Technology includes any information, and only that information, that is not Restricted Data, not available to the public, and "important" to the design, construction, operation, or maintenance of a facility for uranium enrichment, nuclear fuel reprocessing, or heavy water production.

If the information package contains Sensitive Nuclear Technology information, an `<UnclassifiedControlled>` element must be present with a `<Type>` element containing as its element text with single blank character separating all words:

`Sensitive Nuclear Technology`

The following text must appear in the `<Admonishment>` element text:

SENSITIVE NUCLEAR TECHNOLOGY SPECIAL HANDLING REQUIRED NOT RELEASABLE TO FOREIGN NATIONALS

B.4 APPLIED TECHNOLOGY

Applied Technology (AT) is an unclassified category of information established by the Office of Nuclear Energy, Science, and Technology (DOE/NE) to preserve the foreign trade value of certain DOE/NE-funded progress and topical reports containing engineering, development, design, construction, and operation information pertaining to particular programs.

If the information package contains Applied Technology information, an `<UnclassifiedControlled>` element must be present with a `<Type>` element containing as its element text with single blank character separating the words:

`Applied Technology`

The following text must appear in the `<Admonishment>` element text:

APPLIED TECHNOLOGY Any further distribution by any holder of any document or data therein to third parties representing foreign interests, foreign governments, foreign companies, and foreign subsidiaries or foreign divisions of U.S. companies shall be approved by the (insert appropriate NE program office officials), U.S. Department of Energy. Further, foreign party

release may require DOE approval pursuant to Federal Regulation 10 CFR Part 810, and/or may be subject to Section 127 of the Atomic Energy Act.

The specific Office of Nuclear Energy, Science, and Technology positions must be specified.

B.5 COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENT

Cooperative Research and Development Agreement (CRADA) information is data produced in the performance of the agreement that would have been proprietary information had it been obtained from a nonfederal entity.

If the information package contains CRADA information, an `<UnclassifiedControlled>` element must be present with a `<Type>` element containing as its element text with single blank character separating all words:

`PROTECTED CRADA INFORMATION`

The following text must appear in the `<Admonishment>` element text with the CRADA number in (number):

PROTECTED CRADA INFORMATION This product contains Protected CRADA Information, which was produced on (date) under CRADA No. (number) is not to be further disclosed for a period of five years from the date it was produced except as expressly provided for in the CRADA.

B.6 CONFIDENTIAL/FOREIGN GOVERNMENT INFORMATION–MODIFIED HANDLING

Confidential/Foreign Government Information—Modified Handling (C/FGI-MOD) is a controlled information type used to protect foreign government information that must be protected at a level below the level of protection required for information classified Confidential. Assignment to this category can only be performed by a derivative classifier.

If the information package contains C/FGI-MOD information, an `<UnclassifiedControlled>` element must be present with a `<Type>` element containing as its element text with single blank character separating all words:

`Confidential/Foreign Government Information—Modified Handling.`

The / and – characters must not have space characters between them and the words they separate.

The following text must appear in the `<Admonishment>` element text:

This document contains (insert name of country) (insert classification level) information to be treated as Confidential—Modified Handling Authorized.

The name of the country and classification level must be specified.

The information on how the information type assignment was determined is placed in the `<ClassifiedBy>` and `<DerivedFrom>` elements. These element names are the same used to identify the derivative classifier in the `<Classification>` element.

The `<AdditionalInformation>` element is used to contain the foreign government markings.

B.7 CONTRACTOR-OWNED INFORMATION

Contractor-owned information is that which is generated by the contracting company for its use only and needs to be protected from unauthorized disclosure.

If the information package contains Y-12 contractor-owned information, an `<UnclassifiedControlled>` element must be present with a `<Type>` element containing as its element text with single blank character separating all words:

`Contractor-Owned Information`

The – character must not have space characters between them and the words it separates.

The `<Admonishment>` element must be present and contain one of these statements:

COMPANY USE ONLY This document contains privileged information and must be protected from disclosure outside the company unless release is authorized by the Legal Division.

BUSINESS PERSONAL This document contains administrative or employee-sensitive information that must be protected from disclosure to those without a need to know. Disclosure outside the company is prohibited unless release is authorized by the Legal Division.

COMPANY SENSITIVE This document contains administrative or employee-sensitive information that must be protected from disclosure to those without a need to know. Disclosure outside the company is prohibited unless release is authorized by the Legal Division.

B.8 PRIVACY ACT INFORMATION

Privacy Act information consists of certain types of information about individuals such as information that can be used to identify a person, payroll information, medical information, etc.

If the information package contains Privacy Act information, an `<UnclassifiedControlled>` element must be present with a `<Type>` element containing as its element text with single blank character separating all words:

`Privacy Act Information`

The `<Admonishment>` element must be present and contain this statement in its element text:

PRIVACY ACT INFORMATION RESTRICTIONS ON DISCLOSURE This record contains personal/confidential information and is subject to protection by the Privacy Act of 1974; 5 U.S.C. Sect. 552(a). Federal or contractor employees and their subcontractors who willfully make an unauthorized disclosure of information from this record shall be guilty of a misdemeanor and fined up to $5,000.

The name and organization of the person that made the determination is placed in the `<Reviewer>` element text and the date the determination was made is placed in the `<DateReviewed>` element text.

DISTRIBUTION

DOE DISTRIBUTION

R. L. Shoup, LANL

S. Couture, LLNL

A. Russell, LLNL

INTERNAL DISTRIBUTION

C. A. Barton

V. E. Chase

R. L. Crisp

C. G. Holmes

D. M. Kelleher

K. E. Langley

R. A. Lewis

D. J. Linehan

M. D. Love

C. H. Malarkey

J. D. Mason

M. A. McNeil

P. M. Parris

C. H. Richter

R. C. Secrist

R. L. Shipp

R. M. Wilson