Sandia National Laboratories

Exceptional service in the national interest

Need-to-Know (NTK) Considerations for High Volume Data Access

Susan Byrnes, Principal Member of Technical Staff

SANDIA NATIONAL LABORATORIES, NEW MEXICO

May 2022

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. **SAND2022-6253 C**

Background

- Digital Engineering practices are being adopted to accelerate the pace of the Nuclear Weapons Product Realization Life Cycle
- Successful digital engineering practices require timely access to a large number of interrelated artifacts in support of the system engineering life cycle
- In addition to security clearance requirements, access to Nuclear Weapon Data requires verification of the requester's Need-to-Know
- Need-to-Know- A determination that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function (per DOE O 452.8, Control of Nuclear Weapon Data)

Human-intensive team-specific NTK determination processes no longer meet mission needs

Policy / Definitions

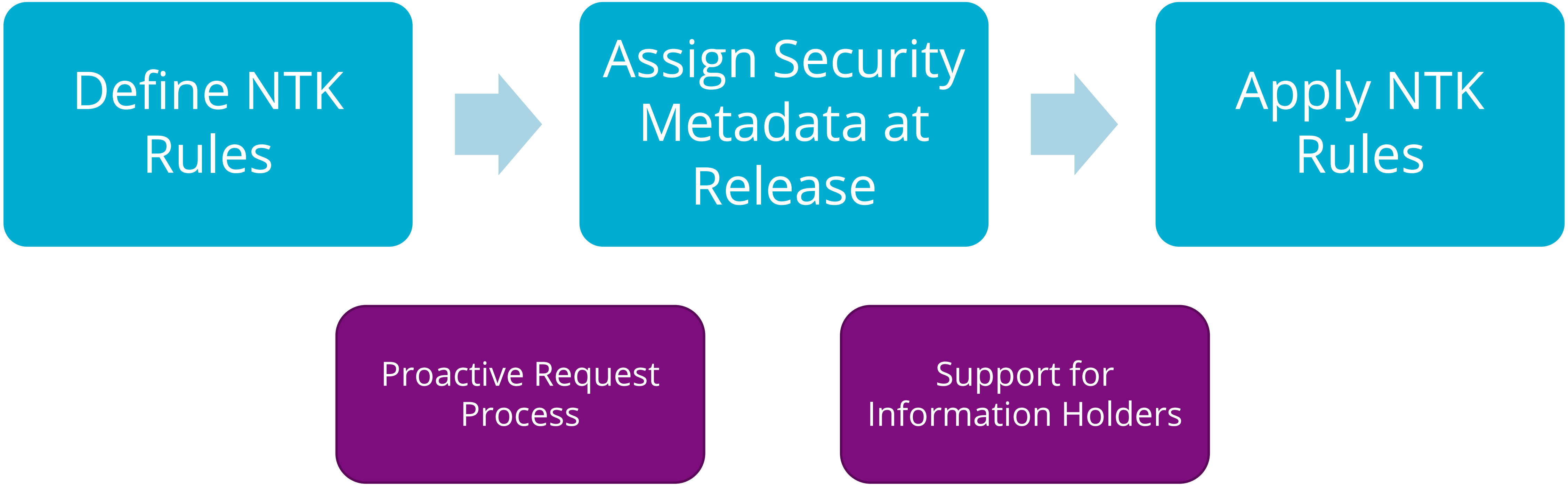
Federal Requirement R010 : Enterprise Need-to-Know

- Defines operating and governance requirements for requesting, evaluating, and provisioning a need to know (NTK) determination to electronic classified information, up to and including SRD. Enterprise NTK applies to electronic classified information created or maintained in Directed Stockpile Work (DSW) funded IT systems for sharing electronically between or among The Nuclear Security Enterprise (Enterprise) sites

SNL RPP-504 : Control of Need-to-Know and Access to Electronic Shared Information

- Information Collection: Information Collections (IC) are virtual containers that establish a consistent NTK for all information within the container. ICs are what individuals request access to and how Information Holders control access to their information.
- Information Holder: A person who makes NTK determinations and provides provisioning (access) instructions for classified nuclear weapon Information Collections

Elements of a Need-To-Know Strategy



Define NTK Rules

Assign Security Metadata at Release

Apply NTK Rules

Proactive Request Process

Support for Information Holders

NTK determinations must balance National Security interests with the effectiveness / efficiency of the workforce

Step 1: Define NTK Rules

Today

New teams define NTK rules for:

- Immediate team-specific access needs
- Preventing access by others

Rules vary by application/repository and NSE site

Product realization life cycle needs of the organization/site and enterprise/complex not a concern

No guidance for sharing

Future

Establish a cross-site, cross-product, cross-discipline team to govern access approaches for the mission

- Encourage sharing
- Discourage exception processing

Re-define information collections that span repositories/applications and sites

Commit to implement across repositories and COTS/custom applications

Step 2: Assign Security Metadata at Release

Today

For many, NTK is “magic” :

- Lack of general awareness for how access is established
- Access control mechanisms are too numerous and complex
- Security metadata is not required or validated in most cases

Result: Data is often inaccessible after release, sometimes even to the author

Future

Transparency and consistency via:

- Cross-site information collections
- Cross-site agreement on security metadata values (using master data values)
- Requiring valid metadata upon data release for use
- Automated selection (or at least validation) of metadata upon release

Result: Intentional NTK assignments

Step 3: Apply NTK Rules

Today

NTK determinations:

- Are often subjective
- Place undue burden on the information holder
- Vary by application/repository and site due to conflicting rules
- Result in multiple follow-on requests for needed access

Future

NTK rules are applied across repositories and sites yielding consistent and predictable results

Valid reasons for access are codified so that more NTK determinations can be made in an automated manner

NTK access provisioned across repositories and sites so fewer access requests are required

Proactive Request Process

- Even within a single team, gaining access to information controlled by that team can be daunting
  - Each repository may require different licensing and access approvals
  - The same data within different repositories is accessible to different people
  - Provisioning is tool-specific, even for the same data
- There is no single place to request and track requests for access
- Providing a proactive request process would provide a "one-stop" shop for requesting access before beginning a new assignment

A common proactive request process would increase productivity by streamlining the request process

Support for Information Holders

- Information Holders are accepting risk every time they authorize access
  - Inaction can sometimes feels like the safest approach
  - There are concerns about the scope of the data involved
  - Following up on ad hoc requests can be time consuming
  - Hand-offs between incoming and outgoing information holders are lacking
- Current Access Renewal Review Process is challenging
  - Renewal process is owned by the information holder rather than the requester
  - Information holders have little insight into individual requester’s actual access patterns over time

Provide appropriate guidance, insight and automation to help information holders with their decision making

Challenges Specific to Digital Engineering

- Deciding the appropriate granularity for making NTK determinations
  - NTK determinations are based on a specific person and a specific *data item*
  - Traditionally a *data item* has been an individual drawing, document or other single data file
  - For digital engineering we need to find the correct granularity for defining data items
    - Each data item needs to be uniquely identified at its source
    - Classified level and category and NTK security metadata apply to the entire data item, so the intended granularity needs to be known at the point the data item is released for use
    - Using too coarse granularity prohibits sharing only a portion of the data item
- Relationships can introduce additional classification and NTK concerns
    - Relationships are the essence and value of the digital thread
    - Classified level and category and NTK security metadata may need to be assigned to the relationships between data items as well as the data item themselves

Other NTK Challenges

- Separating NTK from data creation and modification
  - From a software development or COTS customizer perspective, separating need-to-know from the ability to create or modify data seems counterintuitive
  - However, creating and modifying information are driven by the business processes associated with the information
  - Hands on time for creating / editing ND data is generally very short (1-3 months) compared to the long term need for NTK access to that data (75 years)
  - The individuals involved in creating or modifying data may be dictated by who is available during that brief period in time and may have little bearing on long term NTK access needs
  - Work in process is treated differently for classification purposes as well, once the product is ready for release for general use, the classified level and category (as well as NTK criteria) is applied
- Over-classifying
  - It may be tempting to default all data items in a given classified repository to SRD but this precludes broad sharing of this unclassified but sensitive data

Summary

- Enabling High Volume NTK Access Requests requires an NTK Strategy :
  - Well defined NTK rules based on well defined metadata attributes with well defined values
  - Information Collections that span repositories, applications and sites
  - Requiring and facilitating metadata capture at release time
  - Investment in tools to support information holders and proactive access request processing
- Successful sharing of data requires
  - Commitment from the mission that sharing is essential
  - Collaboration between the mission and IT to ensure feasibility
  - Support for Information Holders decision making