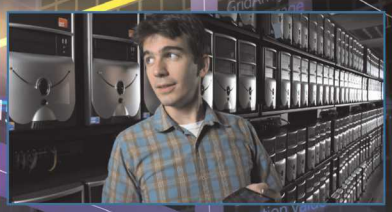
SAND2018-10806R

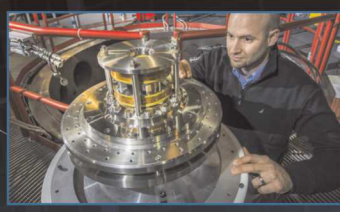
Exceptional service in the national interest

Sandia National Laboratories

NUCLEAR WEAPONS DATA STRATEGY

THE VISION FOR THE FUTURE DATA ENVIRONMENT



Sandia National Laboratories is a multi-mission 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-NA-0003525. SAND2018-5601 O

April, 2018

Sandia National Laboratories

NUCLEAR WEAPONS DATA STRATEGY

Prepared by:
NW Chief Data Officer

Endorsed by:
Office of the Chief Engineer for NW (CENW)
NW Weapon Engineering Council (WEC)

CONTENTS

CONTENTS (continued)

Data is the foundation to accelerate understanding and confidence in the nuclear deterrent, and as such is a key enabler of the success of the NW mission.

Purpose

This document describes the data strategy for the Nuclear Weapons Program Management Unit (NW PMU), with emphasis on functions related to the product realization lifecycle. It describes a vision to more effectively value and utilize data as an asset: data often *is* our product, and when it isn't, our products are made possible only through the data produced and consumed throughout each product's lifecycle. True confidence in the nuclear deterrent requires a clear understanding of how our products perform against requirements; both in the near term as well as over long periods of time. Data is the foundation for this understanding, and as such is a key enabler of the success of the NW mission. This document defines principles that enable a "culture of care" around NW data and drive the specific approaches to create a data-centric environment that is sustainable, agile, and responsive to the needs of the NW mission. The strategy outlined within this document must guide the definition of a high-level roadmap to achieve this vision, which in turn will be supported by separate detailed implementation plans.

Scope

The scope of this data strategy encompasses the data that enables the product realization lifecycle. In this context, data implies all data assets such as databases, documents, images, audio and video files, raw data, models, scripts or code, web sites, data access services, and official electronic records. At this phase, the scope of this strategy is internal to Sandia National Laboratories (SNL) and does not extend to our partners within the Nuclear Security Enterprise (NSE) or elsewhere in industry. However, this strategy may be used to inform interactions with our partners, sponsors, and customers and to manage data obtained from these entities.

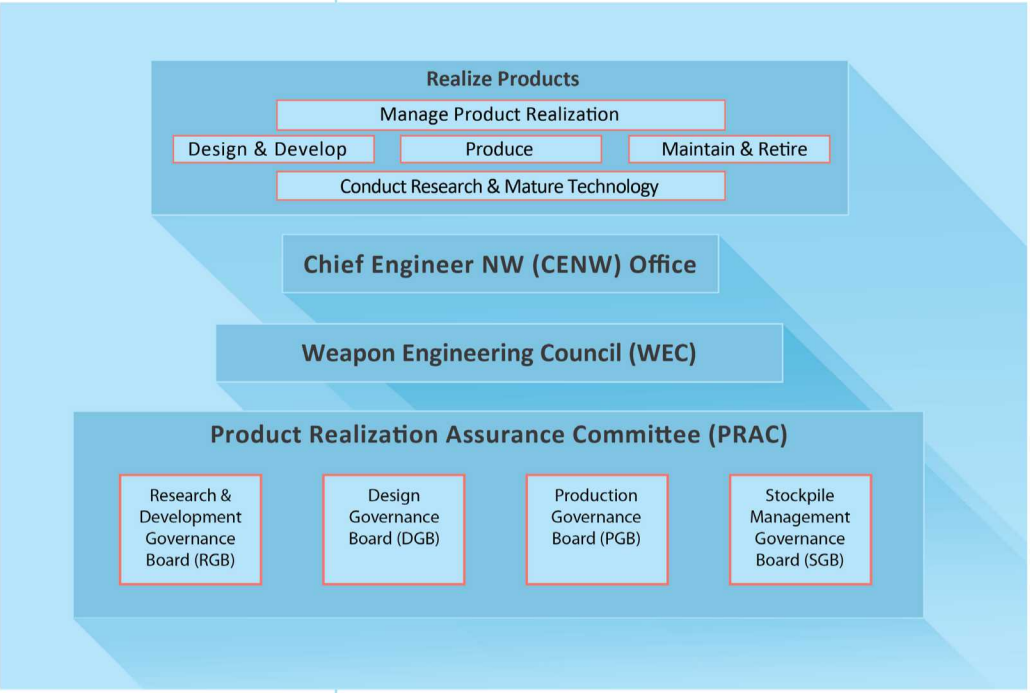


Figure 1: Product Realization Governance Structure

Vision

To meet the demands of the current and future NW mission, the entire range of NW's capabilities and resources needs to be exploited, including our data. This necessitates a shift in the current paradigm from "my data" to "our data." Data must be available and accessible to the largest possible group of authorized users. Currently siloed data sets must instead be readily published and shared. Data governance and infrastructure capabilities must enable data curation and integration at the point of publishing, reducing or eliminating customization and configuration by data consumers. Accessibility includes discovery of data: the data environment must facilitate exposure and discovery, including those relevant data sets that may currently be unknown and inaccessible to a specific user. Although data must be made more accessible, this goal does not seek to undermine appropriate security; data must be protected from unauthorized access at all times. The goal of accessibility will naturally be constrained by information assurance requirements.

Although data must be made more accessible, this goal does not seek to undermine appropriate security; data must be protected from unauthorized access at all times.

NW must transform into a data-centric organization, focused on enhancing knowledge-capture, discovery, and the exploration of ideas. A key paradigm shift is to reduce the burden of data translation and processing on our workforce: data must be understandable and usable by anyone in the authorized community at the time of access. To ensure understandability and usability, data must be governed by data standards that ensure consistency and, when necessary, certain levels of data quality. In addition, an avenue must exist to for users to formalize and "certify" translation and processing routines to be made available to the wider community. Data translation and processing must also be repeatable; appropriate context must be applied to data to allow users to consistently interact with specific data sets. Context is directly related to data provenance, or the what, how, when, where, who, which, and why surrounding data creation and use. Provenance can assist with understanding the uncertainty that exists for any given data set. The NW workforce must be able to readily evaluate uncertainty for any data set. In some cases, specific thresholds of uncertainty for data sets used within critical processes or deliverables must be defined and enforced.

"Modelled on the Open Compute initiative for data centers, Sandia will develop an open environment for internal collaboration on weapon architectures and design concepts on its classified and unclassified networks. Data standards will allow staff to pick the tools of their choice, subject only to maintaining data integrity and openness."
NWMA Strategy 2016, Sustained Deterrence, pgs. 22-24

Data translation and processing must also be repeatable; appropriate context must be applied to data in order to allow users to consistently interact with specific data sets.

Data must also support cohesive decision making throughout the product realization lifecycle, meaning the authoritative source(s) for critical data assets are known, and changes to the source(s) are governed and made immediately available. Furthermore, the community must understand the proper use and meaning for key NW data assets. To accomplish this goal, accountable stewards for governed data entities must be established and a common data dictionary should be openly published and made available to all NW staff.

"**To enable innovation and accelerated development cycles, Sandia will lower barriers to using information resources. Knowledge must be secure, but will be easy to find and use for authorized users.**"
NWMA Strategy 2016, Sustained Deterrence, pgs. 22-24

"**We will address the creation and use of assurance information as an integrated lifecycle challenge.** We will address how we would optimally use different information sources, collectively and separately, to enable agile, risk-informed decision making and let that drive data infrastructure decisions…. Predictive analytics, machine learning and data mining could…allow us to quickly detect hidden patterns, predict behavior, and prioritize work."

NWMA Strategy 2016, Stockpile Evaluation and Assesment, , pgs. 42-43

Data must always be protected; however, NW must rethink the concept of authorization to enable maximum participation from the community. Data security must be designed for flexibility to encourage participation without the risk of inappropriate disclosure. Meanwhile, the release of data to external entities must be governed with clearly defined expectations and rules; data infrastructure should surface these rules and validate compliance for NW staff.

NW will realize the benefit of this vision when our data and the data infrastructure is proactively managed to meet the needs of the mission and the barriers to participate are reduced or eliminated.

Data Principles and Goals

Three guiding principles serve as the foundation for this data strategy and the approaches taken in its implementation. They are core values that will form the basis for all decisions related to data. NW will reinforce these principles through their communications, policies and processes, investments, and partnerships.

1. ***Data is an asset*** *that has value to NW and is governed and managed accordingly.*
   Data is an important corporate resource that has real, measurable value. Corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision making, so we must ensure that we know where it is, can rely upon its integrity, and can obtain it when and where we need it. Data is not all created equal. Its value should be correlated to its use and utility throughout any NW product's full lifecycle. The data with the highest utility to NW is referred to within this strategy as "key data." The identification of key data clarifies why the data is of value to NW and therefore helps to inform decisions.

2. ***Data has assigned stewards*** *accountable for its quality.*
   NW must make the cultural transition from "data ownership" to "data stewardship." Each key data asset must be actively managed by a defined mission area steward to ensure the quality and effective use of that data asset. Data stewards play a core role in defining data standards, representing their community's data needs, educating their community on its data assets, and resolving data issues. As such, data stewards must have the authority and means to manage the data for which they are accountable. The Chief Data Officer will ultimately have accountability for NW data as a whole.

3. ***Data is shared*** *across NW functions and organizations so that users have access to the data necessary to perform their authorized duties.*
   Timely access to relevant data is essential to improving and maintaining the quality and efficiency of the product realization lifecycle. The five goals listed below must be realized in support of this principle.

Data is not all created equal. Its value should be correlated to its use and utility throughout any NW product's full lifecycle.

The third principle, data is shared, can be further elaborated into five supporting goals:

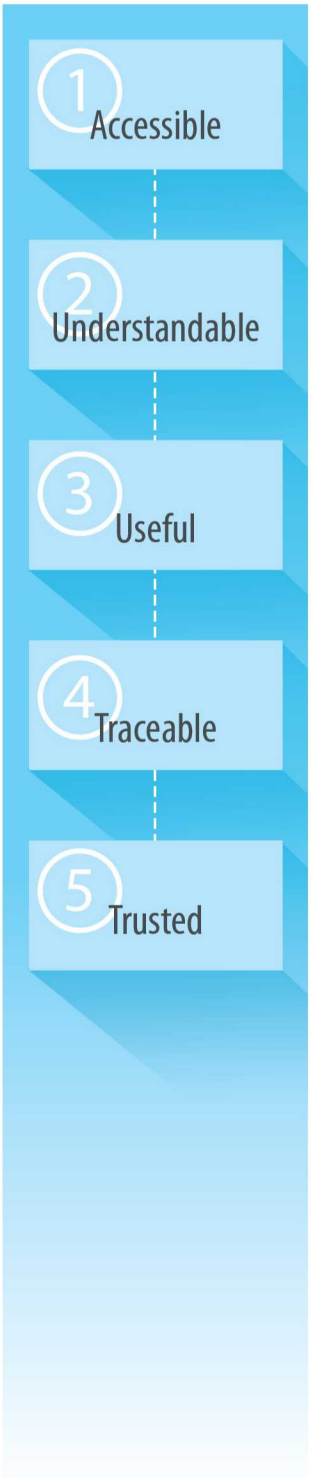
1. *Data is **accessible***
   Accessibility refers to data assets being readily available to authorized users and applications when the data is needed. This includes aspects of availability (where and how the data is stored and accessed), seamless authorization, timeliness of access, and data discovery. Data must have exploitable metadata that allows for its discovery and use independent from where and how it is stored.

2. *Data is **understandable***
   Understandability refers to users and applications being able to comprehend the data, both structurally and semantically, and can easily determine how the data may be used for their own purposes; data must have appropriate contextual information to show how, when, where, and why it was produced, transformed, and used.

3. *Data is **useful***
   Usability refers to data being machine-readable and interoperable, complete, timely in the context of its intended use, and fit for use for all purposes required by the mission. Data storage must be designed with the future in mind; data formats must be flexible and able to adapt over time. Fit for purpose also encompasses the ease with which data is published, accessed, and used.

4. *Data is **traceable***
   Traceability refers to data being able to be connected and linked throughout its lifecycle as well as the product realization lifecycle. Linkage applies not only to tracing the data lineage (its origins, where it moves, and how it transforms over time), but also to different sets of data that are inter-related; therefore, data must be designed to be interoperable. In addition, traceability also refers to linking the data to the operational environment, as in, the processes, requirements, organizations, programs, and people that surround its use.

5. *Data is **trusted and secure***
   Trustability refers to the users' ability to determine and assess the authority of the data's source; that is, the provenance, quality, and authenticity of the data is known and visible, and in some cases, governed. To enable this goal, the data must be properly protected from unauthorized use and disclosure and some data sets must be "certified" for use within specific contexts, as the authority of the data may change based on its use. A consideration for this goal is duplication of data, both in the context of users copying data and in the context of data backup, recovery, and continuity of operations. Duplication of data (and the impact of those processes on the data) should be captured in the data provenance and made visible to the end users of the data.



Future Data Environment

The current approach to storing, accessing, and using data is insufficient to realize the vision described in this strategy. A new data-centric environment must be designed and implemented. Although a new environment is necessary, this does not necessarily imply that all current solutions must be abandoned. Current solutions may continue to be used in the future, but will need to follow foundational standards and rules to participate in the new environment. In fact, it is recommended that standards for the future environment be designed with consideration for the ease with which current solutions could be integrated and brought into compliance. In addition, the NW mission area is not the only organization with a need or desire to more effectively capitalize on its data; the implementation team should reach out to external institutions as well as other mission areas within SNL for best practices and innovative ideas.

"Strategic data management will be enabled by an architecture that truly connects our information collection, storage, retrieval and analysis systems across all lifecycle phases."
NWMA Strategy 2016, Stockpile Evaluation and Assesment, , pgs. 42-43

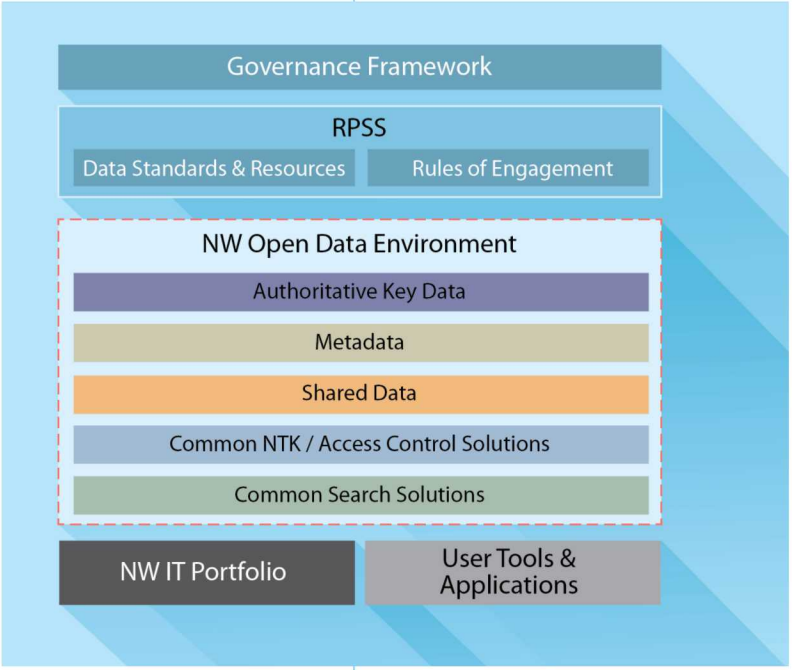


Figure 2: Conceptual view of future data environment

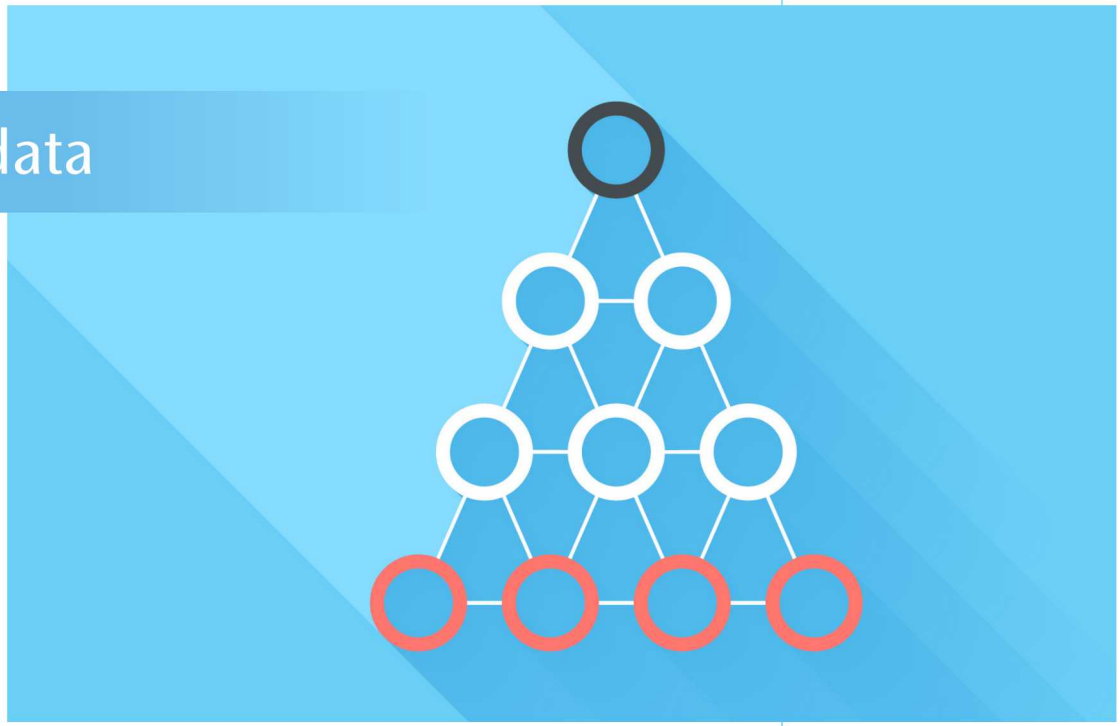
Similar to the guiding data principles and goals, the conceptual view of the future data environment was conceived using five principles as the foundation. These principles should serve as a litmus test for current and future implementation approaches. They are not meant to prohibitively and unnecessarily limit the environment, but rather to guide decision making on possible solutions. Furthermore, NW should facilitate the development and use of common corporate solutions that not only meet NW's mission needs, but the needs of all SNL mission areas.

1. *The data environment maximizes user participation while maintaining proper protection of data.*
2. *The data environment provides data as an open, communal resource, organized within a standardized global structure.*
3. *The data environment is designed for sustainability and optimizes costs.*
4. *Solutions in the data environment leverage industry-supported standards and technologies to improve interoperability and reduce cost.*
5. *The data environment is managed as a critical NW asset.*

Figure 2 shows the conceptual view of a future integrated, data-centric environment. It separates data (and its related properties, such as access controls) from tools and applications. In coordination with key partners, the strategic approaches listed in the next section will realize the vision for this data environment.

Strategic Approaches

1. Govern data



1.1 Establish roles and responsibilities

The data governance framework establishes accountabilities for data, including ownership for this data strategy and its implementation. A new role, the Chief Data Officer (CDO), has been established and will act as the single voice for data to NW's internal and external partners. This role owns the NW data governance function and is accountable for its implementation. The CDO works in partnership with the Weapon Engineering Council (WEC) and the Product Realization Assurance Committee (PRAC) and serves as the arbitrator to resolve data issues. WEC and PRAC own RPSS (Realize Product Sub System), which establishes policy and requirements for the execution of the product realization lifecycle. As such, the data governance framework and its products will be linked to RPSS (more on this under the second strategic approach). The data governance framework also defines responsibilities for stewardship of specific key data sets using data stewards. Data stewards provide local subject matter expertise on data needs and issues and ensure the quality of specific data sets. A supporting set of processes will be defined to inform the key interactions between the various groups involved and to ensure data governance is sustained over time.

Data stewards provide local subject matter expertise on data needs ...

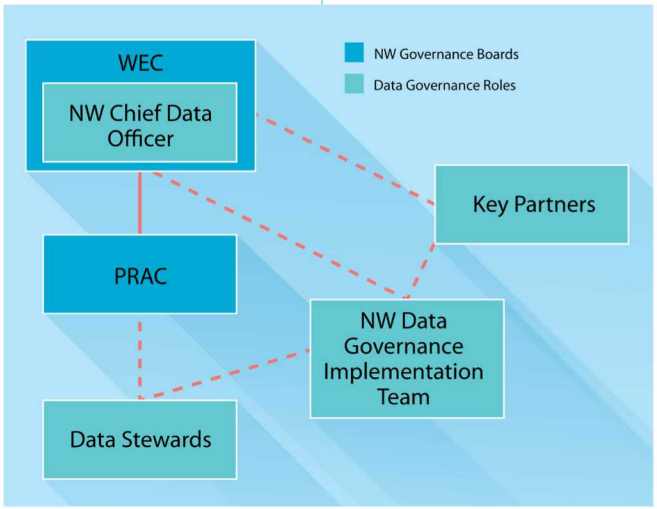


Figure 3: Data Governance Roles & Responsibilities

1.2 Identify and define key NW data assets

The list of key data assets needs to be actively maintained and openly shared with NW staff.

To manage NW's data as an asset, data's value must be correlated to its impact on the NW mission and its core products and services. Criteria must be developed to consistently identify the data elements with the highest impact; "key data." The list of key data assets needs to be actively maintained and openly shared with NW staff. Each key data asset must be assigned a data steward. The data steward is responsible for definition and maintenance of data standards, and for assessing data management practices and data quality. Key data assets will need to be defined (See 2.1, Common Vocabulary) and mapped to where they are produced, stored, and used within the environment.

1.3 Assess maturity of data practices and measure data quality

The data governance function must identify metrics for both data quality and the adoption of the desired data management practices across NW. Once established, key partnerships with the IT organizations and the data stewards will be required to assess and measure the quality of the data and related practices throughout NW. This data strategy and its implementation should be evaluated and revised based on assessment results.

1.4 Institutionalize data practices

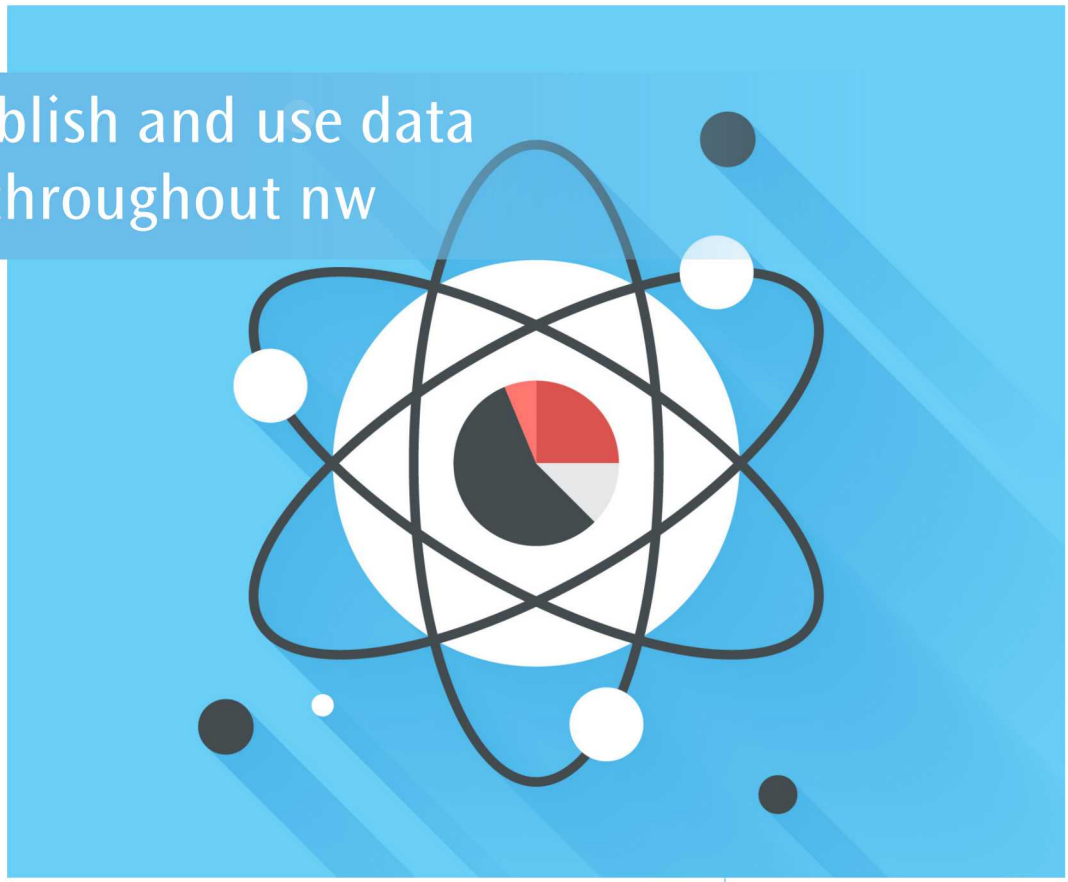
Education efforts must focus staff on their responsibilities with data.

Consistent promotion of NW's data goals and strategy, and awareness of data requirements and standards will reinforce a culture of data stewardship throughout NW. Advocacy must be highly visible and involve all NW leadership levels. Education efforts must focus staff on their responsibilities with data. This is a shift from the current norm to focus education solely on the tools surrounding data. In addition, staff should be shown the benefits of their participation in the data environment. Data stewards should be heavily leveraged in communication and education activities to provide local context to any global NW data standards and practices. In addition, data stewards should be encouraged to implement localized data practices that are in alignment with any global standards and share lessons learned with the broader community.

1.5 Anticipate data needs and optimize investments in the IT Portfolio

One of the key responsibilities for the Chief Data Officer (CDO) is to understand NW's future data needs and, in partnership with WEC and PRAC, prioritize those needs. Ultimately, those needs and priorities should drive NW's data strategy, which in turn should inform and bound investments in the IT Portfolio. The CDO must be the key interface to the CIO and other IT partners and provide a single and consistent voice for the NW community.

2. Define, publish and use data consistently throughout nw



2.1 Establish common vocabulary

Data must be defined consistently throughout NW, and the definitions must be understandable and available to all staff. A common vocabulary is the foundation that enables effective integration and exchange of data. The data governance framework will coordinate and evaluate updates and changes to key data definitions and resolve ambiguities and conflicts between local data definitions through its data remediation process.

A common vocabulary is the foundation that enables effective integration and exchange of data.

2.2 Establish data standards

A clear set of data standards will need to be established and maintained. Necessary data standards include those for data exchange, data publishing, data security, data quality, metadata, and reference data. The data environment must be designed around and optimized for data that conforms to the standards. In addition, NW must focus its investments in the IT Portfolio towards solutions and infrastructure that conform to and enable the data standards, including capabilities that bring non-compliant data into compliance with the standards.

2.3 Publish data resources

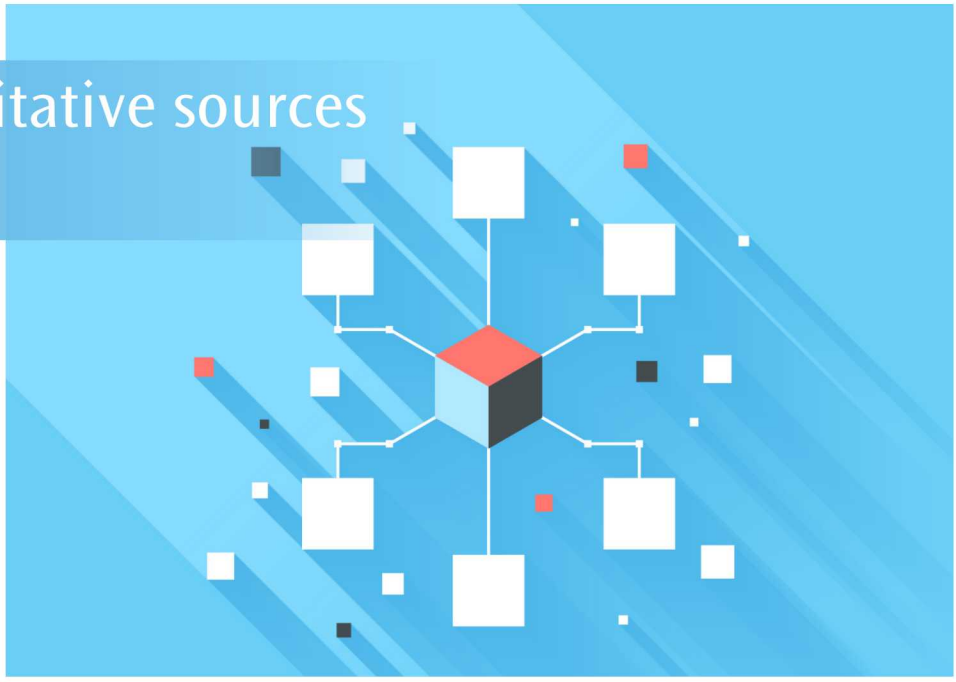
Educational resources should be provided to NW staff, programs, and organizations to support their use of the data environment and to inform programs and teams of best practices for data management, including templates, best practice guides, and

lessons learned. Programs should be provided guidance for how to appropriately staff their information management function, including the appropriate level of resources, necessary skillsets and expertise, and recommended roles and responsibilities. Other important resources will be identified and added as necessary.

2.4 Integrate with RPSS

The standards, resources, and rules of engagement should all be integrated with and accessed through the RPSS framework. Furthermore, RPSS should serve as the basis for the global structures used within the data environment, thus inherently and visibly linking the data produced and consumed throughout the product realization lifecycle to the operational requirements that drive the NW business.

3. Enforce authoritative sources for key data



3.1 Establish and share authoritative key data sets

Data sets that are used across processes, organizations, and/or functions must be published from an authoritative source in an interoperable format.

Approach 3.1 establishes global, cross-cutting data sets that can be centrally sourced and governed. There are two subsets of data sets: managed data and reference data.

Managed data sets are authoritative data sets that are ubiquitous throughout the product realization lifecycle. Each data element determined to be key data in approach 1.2, Identify and Define Key Data, will be analyzed to determine by whom and how that data is used. Data sets that are used across processes, organizations, and/or functions must be published from an authoritative source in an interoperable format. These data sets can then be freely consumed and used by users or tools, thus enabling efficient data integration and ensuring high quality for key data sets. One example of a managed data set is for product structure. Product structure refers to the characterization of a part and its relationships to other parts. For many activities in the product realization lifecycle, it is important to know what weapon and/or component for which the activity was performed.

As such, an authoritative view of the hierarchical product structure for each weapon system should be published and made centrally available.

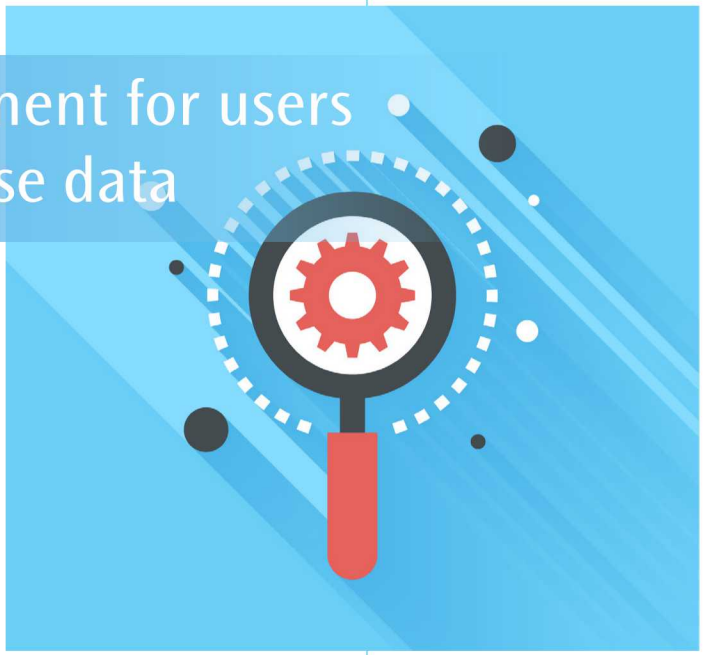
Reference data refers to metadata whose valid values should be controlled to match a central data definition. By using a central list of values, disparate sets of data can be merged at any time without needing to translate and normalize the data values. The Product Realization Integrated Digital Environment (PRIDE) Program currently has a small number of these services available (managed through their Master Data Management project): Weapon Program and System, Person, Site, and Weapon Part and Ancillary Equipment Designation. The intent of approach 3.1 is not to duplicate the effort of the PRIDE Program, but rather to enhance and extend what has already been put into place.

By using a central list of values, disparate sets of data can be merged at any time...

3.2 Require use of authoritative data sets in the IT Portfolio

NW will partner with the CIO's office and IT organizations to establish application development and procurement requirements regarding the use of the managed and referenced data sets in all NW IT solutions.

4. Provide shared environment for users to publish, discover, and use data



4.1 Publish rules of engagement for participation in the data environment

Each user will need to abide by specific "rules of engagement" to interact with the data environment. This ensures each user understands the way data can be published, used, and interpreted within any given structure in the data environment, including expectations around data quality and required levels of rigor for key data sets.

4.2 Store and access data in standard, interoperable formats

The data environment will consist of a combination of actual data assets, metadata registries, and data access services. (Data access services are mechanisms that expose data stored in databases and applications.) Data assets and metadata published in the environment must comply with the data standards established in approach 2.2. In addition, external databases and applications that participate in the environment must comply with the set of accepted data access service methods approved for the environment. This standard set of formats will allow users of the environment to easily access, integrate, and share various data sets.

4.3 Establish the quality of data

Data must be tagged with its provenance and level of uncertainty so that users can appropriately understand and make use of data with varying quality. There is a continuum on which data exists at any point within its lifecycle (Figure 4).

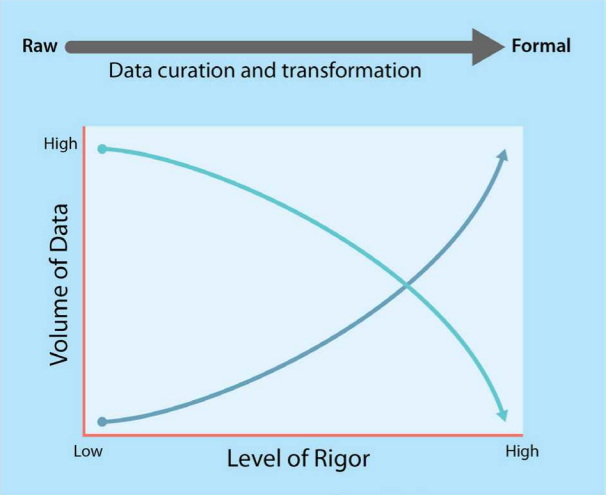


Figure 4: Data Continuum and Level of Rigor

Acceptable bounds of uncertainty for any given data set will be informed by this continuum as well as by the business processes and requirements the data is intended to support at any point in time. The lifecycle of data, and the amount of permutations it experiences throughout this lifecycle, requires a flexible and adaptive approach to handling data quality. Simply stated, the quality of data must be visible to those who use it. Guidance must be established to aid users in evaluating data quality and determining whether it is fit for its intended use. In addition, configuration management processes must control data marked at levels defined as "high quality." Accreditation processes should ensure data sets are being appropriately categorized.

In some instances, where the quality of data must not only be known, but also assured, the data environment must enforce the use of authoritative data sources for these data elements. This could also enforce that key data be stored in a specific location or repository prior to being accredited.

The data environment must facilitate consistent re-use of models, simulations, and analysis whenever possible.

4.4 Enable re-use of data and re-demonstration of processed data

Data must be useful and fit for purpose throughout time. Data formats must be constrained and regulated within the data environment to ensure forward and backward compatibility. When applicable, the raw, unprocessed data must always be stored and made available for future use. Processed data should have metadata that captures the context and assumptions surrounding its translation and processing, including the specific purpose for which the data was transformed and used. The data environment must facilitate consistent re-use of models, simulations, and analysis whenever possible. Where applicable, it should capture why re-use or re-demonstration may not be feasible or recommended.

This set of "self-service" data resources will need to abide by the rules of engagement...

4.5 Allow open participation by users in the data environment

This approach intends to "crowdsource" the build-out of the data environment. A central entity could never, within a short timeframe for low cost, fully understand the users' needs for integrated data sets, scripts, and data analytics tools. Instead, users will be able to publish and share models, scripts, tools, and data sets. This set of "self-service" data resources will need to abide by the rules of engagement and any applicable data standards to be published and shared. In addition, they must be tagged to indicate they are ungoverned and therefore, uncertified. A pathway should exist for user-submitted data and tools to be accredited.

5. Secure data consistently and independent from tools

5.1 Establish common, extensible NTK and access control solutions

This approach allows data authorization to be defined consistently across the organization and IT portfolio rather than being defined separately in every data repository and application. The intent is to establish the requirements for protecting specific data assets once and then publish this mapping in an open format that can be consumed by the applications and tools within the IT portfolio. The current paradigm of applications driving our approach to data security must shift to one where the application portfolio adapts to our rules for data protection and sharing. Solutions must exist to tag and display data security properties on data entities as well as instantiate workflows that allow for proper review and disposition of data security settings. The data authorization approach should be one founded on the principle of inclusion rather than exclusion. We must shift our focus from "need-to-know" to "need-to-share" while staying within the bounds of allowing users access to data necessary to perform their authorized job functions.

Data security should occur at a level that provides flexibility to show users the most relevant data within their need-to-know.

5.2 Associate security metadata with data

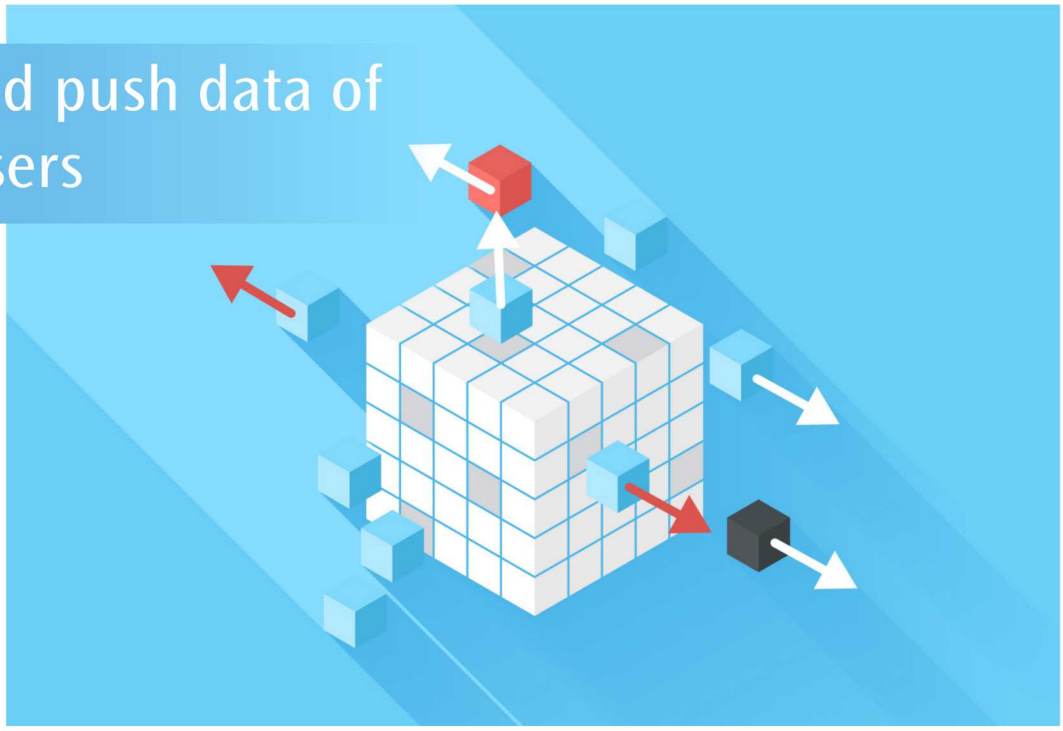
Standard security metadata will be applied to all data within the environment. Data shifts and morphs throughout time and within different contexts; therefore, the metadata must be flexible enough to denote classification, sensitivity, and appropriate use and disclosure throughout the entire lifecycle of the data. In addition, in the anticipated highly integrated environment, the security metadata should be flexible enough to denote the security implications of combinations of data sets.

Standard security metadata will be applied to all data within the environment.

5.3 Require use of NTK and access control solutions in the IT portfolio

NW will partner with the CIO's office and IT organizations to establish application development and procurement requirements regarding data security and the use of the standard NTK and access control solutions in the entire NW IT portfolio.

6. Surface and push data of interest to users



As the data environment matures over time, these search solutions can become more sophisticated and provide artificial intelligence and machine learning capabilities to users.

It is important for the search solutions to work in tandem with the access control solutions to provide appropriate data to ***authorized*** *users.*

6.1 Establish common, extensible search solutions

The future data environment will require a robust suite of search solutions that enable data published within the environment to be discovered. As the data environment matures over time, these search solutions can become more sophisticated and provide artificial intelligence and machine learning capabilities to users.

It is important for the search solutions to work in tandem with the access control solutions to provide appropriate data to *authorized* users. However, to accelerate cycles of learning, the search capability should surface the existence of data that is currently inaccessible to users while maintaining necessary controls around sensitive metadata or the data itself. The environment should seek to answer for users, "what *should* I know"?

6.2 Associate discovery metadata with data

To facilitate the discovery of data within the data environment, users and applications must provide discovery metadata associated with all data published to the environment. A common set of discovery attributes will be established; local sets of attributes may also be established to complement and enhance discovery of specialized data sets.

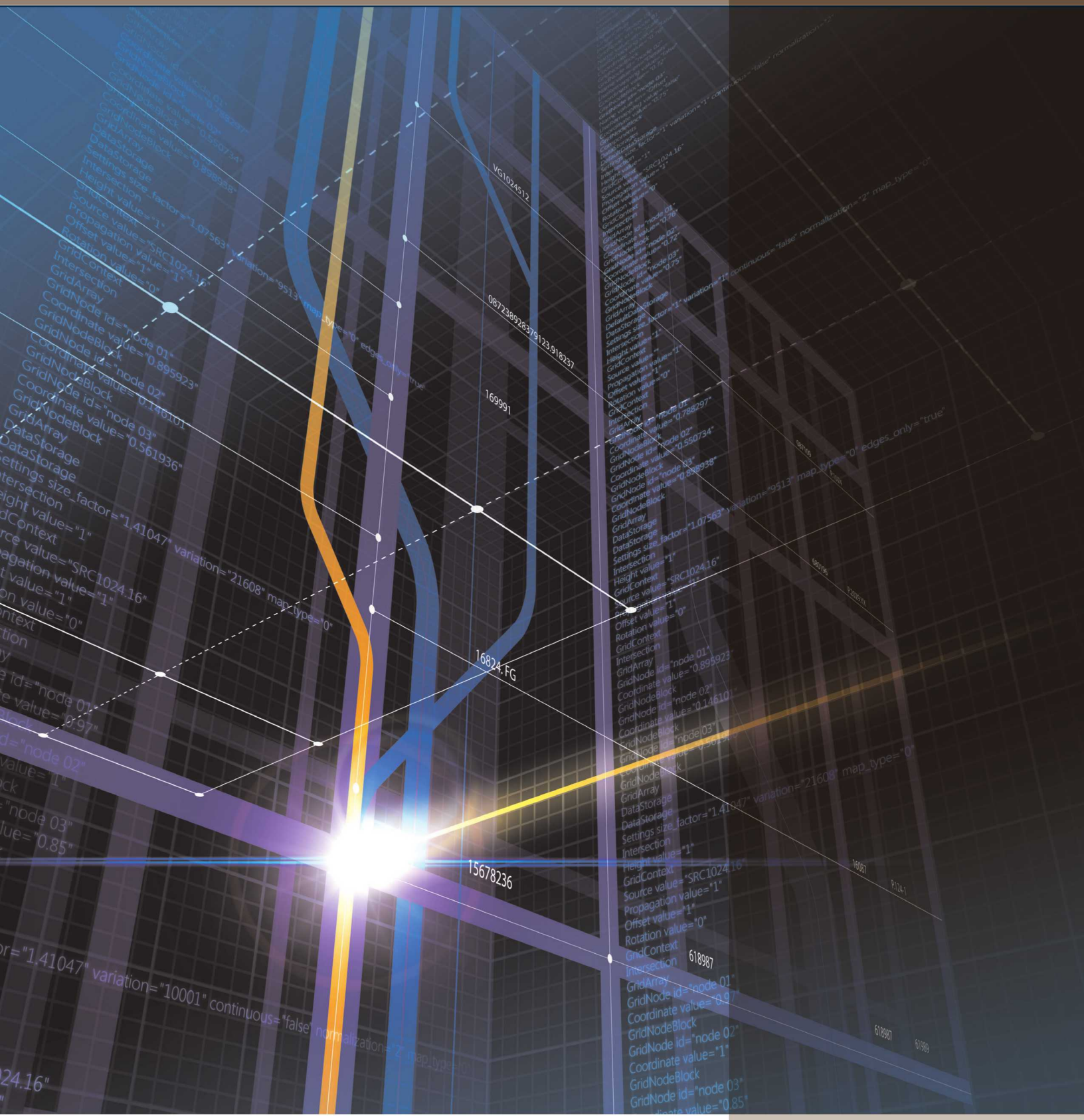
7. Conclusion

Data is the foundation for executing and accelerating the NW product realization lifecycle, and grounds our confidence in the nuclear deterrent. Implementing the approaches defined in this document will better enable SNL to more effectively utilize and value data as an essential asset, but it will require partnerships and collaborations that may not naturally occur within NW or SNL. The success of this strategy depends on active participation from the CENW's Office, NW senior leadership and governance boards, Systems Engineering Technical Processes (RPSS) team, CIO's Office, mission and enterprise computing organizations (including high-performance computing), data science and analytics communities, Classification Office, and even our sponsors and customers where policy or requirement changes may be necessary. The success of this strategy also depends on foundational changes to business practices within the product realization lifecycle as well as the data and computing environment that supports NW, thus requiring sustained commitment, investment, and leadership from all levels of NW and SNL management. While this strategy is intended to establish a vision that can be achieved over many years, it should be seen as a living document that can be refined over time. Execution of this strategy will be supported by an implementation roadmap and detailed implementation plans, the success of which will be judged by the sustainment of a robust "culture of care" around NW data.

The success of this strategy also depends on foundational changes to business practices within the product realization lifecycle as well as the data and computing environment that supports NW

Appendix A: Future Value Statements

Data is a core NW asset and it has an enduring mortgage that must be met.
Sustained leadership and ownership exists for the data strategy and data environment.
Data is stewarded throughout the product lifecycle.
Our workforce will experience a first day on an assigned project in which they will have seamless access to the data and tools they need to do their job.
Data is readily shared and available to a broad set of users allowing different "lenses" to view and use the data.
Data is protected, but access to data within a person's authorization level is seamless; the method by which data is authorized is also seamless.
Our workforce knows where to find data and whether or not it is the right data to use.
The entire data lifecycle is considered at the beginning of any program/project.
The pedigree of data is understood and maintained.
Data environment facilitates exposure and discovery, including those relevant data sets that may currently be unknown and inaccessible to a specific user.
Data environment costs are optimized.



U.S. DEPARTMENT OF ENERGY

NNSA
National Nuclear Security Administration

Sandia National Laboratories