

Building an Interoperable HBOM Ecosystem for Energy Sector Supply Chain Security

By Allan Friedman and Nicholas Leiserson

Supply-chain security is increasingly recognized as an important element of national security.¹

Supply-chain compromises involving trusted technology providers and other third parties have shown how adversaries can gain access to sensitive systems, while attacks on electricity and fuel infrastructure have demonstrated the potentially severe consequences for the energy sector.² The 2026 Executive Order on securing the United States bulk-power system³ addresses a core element of this national security problem: the security and resilience of critical equipment may depend not only on the equipment manufacturer, but also on the underlying components, software, firmware, sub-assembly manufacturers, and supply-chain relationships.

Bulk-power equipment, like much of critical infrastructure, is complex, long-lived, and dependent on global supply chains. Risk can arise from hidden functionality; counterfeit or substituted components; malicious hardware implants; overly-concentrated sources of supply; foreign control over maintenance or updates; or an inability to replace critical components during a crisis. A policy focused only on final assembly, the prime contractor, or the label on a finished product will miss some of these risks. An approach that treats all foreign content as equally dangerous, on the other hand, would impose substantial costs without necessarily improving security.

To successfully implement the EO, the Department of Energy (DOE) needs more than a list of prohibited entities or countries. It needs a sustainable way for manufacturers and their suppliers, asset owners, and government analysts to understand what is inside relevant equipment, where it came from, what remains unknown, and how much confidence to place in that information. Hardware bills of materials, or HBOMs, should therefore be part of the implementation strategy for the EO.

This paper presents a vision for an interoperable HBOM ecosystem serving the energy sector and other critical infrastructure. It concludes with recommendations that treat confidentiality, practical implementation, and cross-sector reuse as design requirements from the outset.

Begin with a shared definition of HBOM

A “Bill of Materials” is not a new concept in industry. Manufacturers of almost all physical systems have long used bills of materials to support design, procurement, manufacturing, assembly, and logistics. These “manufacturing bills of materials” are a necessary step for understanding some aspects of the supply chain, but on their own, they will not result in a detailed understanding of supply chain risks. There are three key limitations in widely used manufacturing

bills of materials. First, they are largely designed and understood as internal data, fit for purpose for the specific manufacturer, rather than a customer or regulator. Relatedly, they often do not have full supply chain visibility into the underlying components in sub-assemblies or into the transitive supply chain dependencies. Finally, they may not have detailed provenance data about the origins and ownership of components.

Building on the experience and growing use of software bills of materials (SBOMs), “HBOM” is increasingly used

About the Institute for Security and Technology

The Institute for Security and Technology (IST) is the 501(c)(3) critical action think tank that unites technology and policy leaders to create solutions to emerging security challenges.

IST stands at the forefront of convening policy-makers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national se-

curity and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

to describe something distinct from commonly used manufacturing bills of materials. However, even as use of the term “HBOM” has increased, there currently exists no consensus on what this term means. For the purposes of this paper, an HBOM is understood as structured information about hardware composition and provenance that can be shared across supply chains and with customers to support security and other risk analysis.

A shared comprehensive and actionable definition of HBOM should identify the core purpose and boundaries of the concept without attempting to settle every implementation question at the outset. It should establish a scope of what would be expected to be covered by an HBOM, the types of supply chain data that might be included, and an understanding of the provenance data needed to inform specific risk-based decisions. At its core, an HBOM should provide structured information about the physical components in a product, the relationships among those components, and relevant provenance. It should also communicate its own scope, including the level of component detail represented and the extent of the available provenance information.

Shared definitions make regulatory and procurement requirements more straightforward. They also support a more effective and competitive tooling and services market. Customers can understand what different offerings produce, compare those offerings against common expectations, and combine tools designed for different needs. Tool developers can innovate without having to persuade every customer to adopt a new meaning of “HBOM.”

The goal should not be a centralized government database or a single mandated technical platform. It should be a common vision for hardware supply-chain transparency, that can then be supported by interoperable data, practical disclosure models, and an evolving ecosystem of tools and services.

Build on the successes— and limitations—of SBOM

Software bills of materials provide the closest precedent. SBOMs have demonstrated value in [vulnerability response](#), [dependency analysis](#), [end-of-life tracking](#), [licensing analysis](#), [procurement](#), and [broader software supply-chain risk management](#). An SBOM does not determine whether a product is exploitable or operationally important; it helps identify potentially affected products and focus limited analytical resources.

An HBOM can play a similar role. It should provide structured information that can support different forms of analysis without attempting to encode specific risk judgments into the inventory itself. For example, SBOMs should enable a user to map components to a list of vulnerabilities, rather than actually including the vulnerabilities themselves in the SBOM metadata.

The maturation of SBOM also demonstrates the value of an open, multistakeholder process. Work done by the National Telecommunications and Information Administration (NTIA) in the mid-2010s brought together software producers, customers, open-source communities, researchers, toolmakers, government agencies, and other participants from across the supply chain. That process helped identify useful baseline information, realistic implementation practices, unresolved questions, and costs that would otherwise have been easy for policymakers to overlook. By 2021, NTIA released a minimum elements document that has formed the basis for SBOM adoption, and subsequent guidance issued by the Cybersecurity and Infrastructure Security Agency (CISA) has continued to evolve based on stakeholder feedback and implementation experience.

A thriving and still-evolving tooling ecosystem has grown around that common vision. [Open-source tools, venture-backed startups, and established security and enterprise-software vendors](#) address different needs, including SBOM generation, validation, enrichment, vulnerability correlation, storage, exchange, procurement, and policy enforcement. No single tool performs every function. The ecosystem works because multiple tools can produce, consume, or enrich sufficiently interoperable information to meet the needs of internal application security teams, product security teams, potential customers doing risk analysis, and software operators responding to new vulnerabilities and security incidents.

In 2026, SBOMs have demonstrated clear value across sectors and industries, but SBOM implementation remains imperfect and nondeterministic. Different tools may identify different components. Dependency relationships may be incomplete. Product identity and versioning remain difficult. Organizations are still learning how to integrate SBOM data into operational decisions. These limitations should inform the development of HBOM. Initial requirements should be useful but capable of evolving as implementation experience, standards, and tools mature.

Adopt a “BOM mentality”: inventory first, interpretation second

The ultimate goal of an HBOM ecosystem serving the energy sector and other critical infrastructure is to address supply chain risk. That risk is not as simple as saying everything from one country of origin has the same level of security risk, or that every source organization or link in a chain of custody impacts an asset owner the same way. It is up to policymakers and individual organizations to determine which specific risks to care about, and what level of risk appetite to accept.

For example, it may not be the case that every Chinese component in a system poses a real risk. In some cases, one can judge that the component type and context simply cannot affect the security of a system. In many other cases, however, making that determination requires knowing the origins of

components. Understanding component type and context about its origins both require an HBOM. After understanding the product and its components, risk judgments should be applied to each data point separately.

HBOM data include component identity, relevant supply-chain relationships, and provenance. Provenance belongs in the HBOM because it describes the component and its history: who produced it; where relevant manufacturing or transformation occurred; and how it entered the finished product. Those facts may be difficult to establish, and different assertions may carry different levels of confidence, but they remain facts about the component.

Whether those facts create unacceptable levels of risk is a separate question. The same component and provenance data may support analyses concerning foreign influence, counterfeiting, tampering, single-source dependency, obsolescence, quality, trade compliance, or other policy concerns. Different agencies and customers may apply different risk criteria to the same information, or have different thresholds of what is acceptable.

The same pattern is visible in SBOM. One inventory can support vulnerability analysis, end-of-life tracking, open-source maintainer risk, and license compliance. The inventory does not need to be recreated when the question changes.

DOE should preserve this separation. Policymakers should set a risk appetite and prioritize threats. Analysts should evaluate risk to see if it meets or exceeds that appetite. An HBOM's role is to provide the data to feed that analysis, including the components, provenance, and relationships. Evidence and assurance processes should then work to establish confidence in those assertions. A shared HBOM approach, ultimately supported by standards, will enable a range of risk analysis and mitigation policy and practices.

Distinguish component coverage from component provenance

To understand the supply chain of a given product, we must determine which components are present in the system and what we know about the origin, production, and handling of each component.

Component coverage describes how much of the product's physical composition is represented in the HBOM. Coverage depends on the declared scope and level of granularity. An HBOM might cover all field-replaceable units, all assembled boards, all active electronic components, or a more detailed set of parts. A claim of completeness is meaningful only if it identifies the level at which completeness is being asserted.

Provenance describes what is known about the origin and production history of each component represented in the HBOM. This may include the component manufacturer, manufacturing location, direct supplier, distributor, contract manufacturer, or relevant production and assembly steps. Any supplier, facility, or production step should be explicitly linked

to the component, subassembly, batch, or product instance to which it relates. Provenance can also cover custody, handling, and movement.

An HBOM can therefore have broad component coverage but shallow provenance. It can also contain extensive provenance for a few selected components while providing poor coverage of the product as a whole.

This distinction allows DOE to separate two policy objectives. Broad coverage creates visibility into what is present. This transparency enables prioritization, particularly when mapped to the functionality of a given set of components in a system. Deeper provenance is complementary. It supports investigation of components that could create significant risks. DOE need not require maximum provenance depth for every resistor, fastener, or commodity part to require that components within a defined scope be represented.

Broad coverage matters even when many listed components do not appear to present an immediate risk. Enumeration of components is separate from the risk analysis step, since policy or the threat landscape may change over time. A component considered unimportant today may become relevant when a supplier is sanctioned, a vulnerability is discovered, a counterfeit campaign is identified, or new threat information changes the analysis.

Coverage also establishes a baseline against which unexpected or undocumented components can be identified. While a given component's role may not be explicitly clear from the HBOM itself, its presence in an HBOM shows that all parties present are aware of it. This can avoid the risk of undocumented hardware components.

An undeclared communications module, debug interface, processor, sensor, storage device, or remote-management capability may be important even if it does not match an existing government watchlist. Origins matter, but security is about more than provenance. Especially in critical infrastructure, risk analysis should consider whether a system can share data, communicate with unauthorized parties, or perform functions that the asset owner does not understand or control. An HBOM itself will not independently reveal a physical component omitted from the manufacturer's declaration. Inspection, testing, teardown, or other validation may still be necessary. The inventory nevertheless makes the discrepancy identifiable by enabling comparison among the as-designed, as-built, as-declared, and, where available, as-observed configurations. DOE can use the nature and security significance of those discrepancies, together with system criticality, provenance, and the assurance supporting the available information, to prioritize further investigation, mitigation, or enforcement rather than treating every discrepancy as equally risky.

After establishing appropriate coverage, DOE can apply risk-based requirements for provenance depth and assurance. Components with the ability to influence control, protection,

communications, configuration, updates, safety, or recovery may warrant deeper tracing. The same may be true for components associated with common-mode failures, concentrated sources of supply, difficult replacement, or plausible pathways for persistent access.

Foster an interoperable HBOM ecosystem

Once policy objectives have been laid out, the question becomes: how challenging is it to produce data to satisfy them? Much of the information needed for an HBOM already exists. It is distributed across engineering systems, enterprise resource planning platforms, product-lifecycle management tools, manufacturing execution systems, quality-management systems, supplier portals, procurement records, and proprietary databases. Different organizations may describe the same component differently, and important context may be embedded in documents or understood only by particular employees.

DOE should not require manufacturers to replace these systems or reconstruct the same information separately for every regulator and customer. The objective should be an ecosystem in which relevant data can move among existing tools and representations without requiring wholesale rewrites or extensive explanation.

Interoperability does not require every organization to use the same internal system or data model. It requires enough agreement on meaning, identity, relationships, provenance, scope, and evidence for one system to interpret information produced by another.

Government can help establish that common vision by defining the decisions that HBOM information should support and the basic concepts that should be represented. Note that this step is still earlier than establishing a “Minimum Elements.” Before the mandatory data fields can be established, we need a clear, shared understanding of goals and use cases. This can then enable a discussion around specific types of data that may be represented in the HBOM. Industry, standards organizations, open-source communities, and commercial providers can then develop different ways to produce, exchange, validate, manage, and analyze the data.

This model supports competition. It gives established enterprise vendors a basis for adapting existing products, allows startups to focus on underserved problems, and enables open-source tools to test new approaches or provide broadly available reference implementations. A clearer market also helps manufacturers and other potential customers distinguish among supply chain products that generate an inventory, validate supplier claims, manage HBOMs, provide provenance evidence, or conduct risk analysis.

Place responsibility where the information is created

In general, equipment manufacturers should be responsible for producing and maintaining the HBOM for the product they design and sell. In the context of the Bulk Power EO, this means that creators of “bulk-power system electric equipment” would be responsible for producing and maintaining those HBOMs. However, this does not assume that manufacturers currently have access to all of this data. The underlying information will originate across the supply chain: component suppliers provide component and provenance data; board and contract manufacturers record production and substitutions; and the original equipment manufacturer or system integrator combines that information into a product-level HBOM. The entity responsible for the finished product may not be able to independently verify every lower-tier assertion, but it is generally best positioned to assemble the information, identify its sources and limitations, and provide it in a usable form.

Bulk-power asset owners and operators have a different role. They should identify the products and configurations deployed in their environments, associate the relevant HBOMs with their asset inventories, and record field modifications, replacements, and operational context.

Placing the principal HBOM-production burden on each generator or utility would produce inconsistent results and duplicate work across customers purchasing the same equipment. It would also favor the largest asset owners, who have greater leverage over suppliers, while leaving smaller utilities and operators with less visibility. DOE requirements should create a reliable path for product-level information to move downstream, while assigning the task of collecting deployment-specific and operational information to the organizations that possess it.

Keep HBOM distinct from functional and operational information

The RFI appropriately asks about remote access, maintenance services, updates, software, firmware, digital services, and other mechanisms through which equipment may affect the bulk-power system. These are important risks, but they should not all be placed inside the HBOM.

An HBOM should identify relevant physical components and their provenance. It might identify that a product contains a particular communications module, processor, modem, wireless chipset, or management controller. Whether that component is enabled, externally reachable, connected to a particular network, or capable of receiving remote commands is functional or operational information.

The same distinction applies to updates. An HBOM might identify the hardware supporting a firmware update process, while an SBOM or firmware BOM identifies the relevant code. The party authorized to deploy updates, the network path

used to deliver them, and the conditions under which the equipment accepts an update belong in linked system or operational records.

DOE should ensure that this information can be associated with the relevant equipment and components. It should not expand HBOM until the term becomes shorthand for every fact that might be useful in a product-security assessment. Clear boundaries make the data easier to create, maintain, exchange, and reuse.

Represent coverage, gaps, and unknown information explicitly

An HBOM must communicate the boundaries of the information it contains. Especially in the early stages of supply chain tracking practices, HBOMs will not be complete. This must be explicitly documented.

The producer should identify the scope of the HBOM, the methods used to generate it, the level of component coverage, the provenance data available, and any known limitations.

The representation should distinguish information that is known and disclosed from information that is known but withheld. It should also identify information that is unknown to the author, was not investigated, falls outside the declared scope, or may no longer be current.

This principle was built into SBOM work from the beginning. NTIA's 2021 minimum elements addressed "Known Unknowns," and subsequent CISA work refined the treatment of coverage and unknown or withheld information. Gaps will exist, but must be documented.

An organization cannot enumerate literal "unknown unknowns." It can, however, disclose the boundaries and methods of its inquiry, acknowledge that unidentified components or relationships may remain, and state the confidence that a recipient should place in the result.

DOE should require HBOM assertions to distinguish "not present" from "not known" and "known but not disclosed." As the data models mature, additional approaches could address information that was "not examined" or falls "outside scope." DOE should also avoid using a single completeness label that conflates component coverage with provenance depth.

Design confidentiality into the HBOM ecosystem

Manufacturers and suppliers will have legitimate concerns about disclosing detailed hardware composition and provenance. This challenge is likely to be greater for hardware than it has been for software. The SBOM development process coordinated by the U.S. government [expressly acknowledged intellectual property and confidentiality concerns](#), but in practice, this has mostly been addressed by not making SBOMs fully public. While software

does have long and complex supply chains, much of the upstream supply in modern software is built on open-source projects, rather than nested layers of proprietary systems with trade secrets. Software also exposes more data in its digital form: software components can often be identified through binary analysis, package metadata, public repositories, and license notices.

We should expect confidentiality to be a bigger concern for HBOM. A detailed hardware inventory can expose proprietary product architecture, supplier relationships, manufacturing locations, sourcing strategies, capacity constraints, alternate sources, and commercially sensitive design decisions. In many cases, it is the supply chain relationships themselves that companies wish to protect. Hardware supply chains may depend on a small number of specialized suppliers, making individual relationships easier to infer. Products may remain in service for decades, extending the useful life and sensitivity of disclosed information. Lower-tier suppliers may also be unable or unwilling to provide information because of contractual restrictions or their own commercial interests.

These concerns do not weaken the case for HBOM; they mean that transparency should not be equated with unrestricted public disclosure. Confidentiality should be treated as a design requirement for the HBOM ecosystem, rather than an exception to an assumption of public disclosure. At the same time, confidentiality cannot become a blanket reason to provide no useful transparency.

DOE should begin by defining what regulators, purchasers, and asset owners need to accomplish. For each use case, the government should identify the necessary facts or assurances, the parties that need access, the appropriate level of detail, the timing of disclosure, and the evidence needed to trust the result. It should also consider whether the recipient needs the underlying data or only an auditable answer to a defined question. Note that this process should not be exhaustive. The short term priority should be to focus on concrete, immediate use cases.

Once those requirements are clear, government can facilitate an open process for industry and the technical community to explore implementation. Possible models include direct disclosure under access controls, auditable attestations, trusted third parties, data escrow, controlled queries, confidential computing, zero-knowledge techniques, distributed records, or combinations of technical and institutional safeguards. DOE should not assume that one mechanism is appropriate or mature for every use case.

A multistakeholder process can evaluate feasibility, cost, scalability, evidentiary value, and new risks created by different approaches. Manufacturers, lower-tier suppliers, asset owners, regulators, tool developers, standards organizations, and confidentiality experts will each see constraints that others may miss.

The objective is purpose-specific disclosure: providing

the information or assurance needed for a decision while protecting data that the recipient does not need to possess.

Levels of HBOM requirements

Not all HBOMs need to be the same. We should expect HBOM requirements to differ across products, sectors, and use cases. The security concerns and potential national security consequences associated with consumer electronics, medical devices, telecommunications infrastructure, and defense technology clearly differ. Risk can also vary within a sector based on a product's function, deployment, criticality, and consequences of compromise.

There is a clear cost to collecting detailed component inventories and provenance information, maintaining that information over time, and producing the evidence needed to support confidence in it. As a result, graduated HBOM requirements will be needed that align component coverage, provenance information, validation, and lifecycle obligations with the product's criticality, the decision being made, and the consequences of relying on incomplete or inaccurate information. More demanding requirement levels should apply where the expected security benefit justifies the additional cost and complexity. These requirements should be a finite set of levels that gather requirements for coverage, provenance data, and assurance of that data.

DOE should use a risk-based analysis to determine the appropriate levels of requirements. Higher-consequence products or even components may require information about lower-tier suppliers, manufacturing locations, contract manufacturers, ownership or control, and relevant transformations. They may also require stronger evidence, independent validation, or continued monitoring.

Coverage depth and assurance are two further dimensions that should remain distinct. Coverage depth concerns how far the supply chain has been traced. Assurance concerns the confidence that can be placed in the resulting information. A direct-supplier assertion and an independently verified manufacturing record may describe the same provenance claim but provide different levels of assurance.

The RFI uses "sub-tier" and "depth of tracing" to describe how far an inquiry extends into the supply chain. DOE should preserve those terms for supply-chain depth and use a separate concept, such as "data assurance," for evidence quality.

This framework avoids accepting unsupported assertions for consequential equipment while also bypassing expensive verification of every component without regard to function or impact.

Link SBOMs, HBOMs, and other BOMs while allowing each to evolve

Modern equipment cannot be understood through hardware information alone. Hardware, software, firmware,

cryptography, AI models, data, and services interact to create the behavior and risk of the system.

SBOMs, HBOMs, cryptographic bills of materials, AI bills of materials, and other transparency artifacts should be capable of referencing one another. Common product and component identifiers, version information, and explicit relationships can help an analyst transition from assessing a physical component to its firmware, from firmware to its software dependencies, or from a cryptographic implementation to the product in which it operates.

These BOM types should not yet be forced into one comprehensive artifact or schema. They are developing through different communities, at different levels of maturity, and in response to different use cases. Binding them too tightly now could slow adoption and freeze assumptions that will need to change.

The near-term objective should be linked, composable information. A "crawl-walk-run" approach would begin with useful domain-specific BOMs that have clear scope and reliable identifiers. The next stage would link those artifacts and allow relevant tools to exchange or jointly query their data. Over time, this could support integrated analysis across hardware, software, firmware, cryptography, AI, and other supply-chain information without requiring every source system to adopt one representation.

Each BOM community should be able to refine its data and practices as use cases and tools mature. Interoperability should make that evolution easier rather than constraining it.

Treat HBOM as lifecycle information

Bulk-power equipment may remain deployed for decades, but its component composition and supply-chain risk will not remain static.

Manufacturers routinely substitute assembled boards or individual components based on cost, availability, lead times, and production needs. These substitutions may satisfy the manufacturer's technical and quality requirements while introducing different manufacturers, new manufacturing locations, lower-tier suppliers, or changing levels of available provenance data. Two units sold under the same model number may therefore contain technically equivalent components with materially different supply-chain histories.

An HBOM must be associated with a sufficiently specific product configuration. Depending on the product and use case, that may mean a model version, production lot, serial number, board revision, or other configuration identifier. DOE should not assume that one product-family HBOM accurately describes every unit produced over many years.

Suppliers also change, companies merge or cease operations, software and firmware are updated, and new threat information alters the significance of existing components. Maintenance and refurbishment can introduce further substitutions after deployment.

A lifecycle approach does not require every recipient to receive every update immediately. It requires a durable method for connecting a particular asset to the information that accurately describes its configuration.

Build for cross-sector and whole-of-government use

Manufacturers affected by the bulk-power Executive Order often serve multiple sectors. They are already responding to overlapping requirements concerning hardware components, supplier identity, country of origin, and provenance.

The FCC's [Covered List](#) and equipment-authorization proceedings affect communications equipment and have directly addressed the treatment of component parts. Commerce Department rules restrict certain connected-vehicle hardware and software components linked to China or Russia. Defense procurement includes restrictions concerning telecommunications equipment, printed circuit boards, and other designated components or sources. Federal contractors across the broader government market must address Section 889 representations, Section 5949 semiconductor restrictions, and prohibitions concerning covered telecommunications and video-surveillance equipment and services.

Energy, medical devices, aerospace, industrial automation, AI infrastructure, data centers, and other connected-product markets are responding to similar concerns through standards, customer demands, procurement practices, and emerging regulation.

These regimes serve different policy objectives, but they repeatedly depend on overlapping information.

A manufacturer should not have to rebuild its supply-chain records for each agency, sector, and customer or be forced to represent the same provenance fact through incompatible systems.

DOE should therefore coordinate with other federal agencies and standards communities to maximize reuse of identifiers, provenance concepts, evidence, and exchange mechanisms. Each agency can retain its own statutory authority, risk model, and decision criteria while drawing on a common foundation of interoperable information.

Without coordination, government will continue to create one-off attestations and contractual flow-downs that are costly to produce, difficult to validate, and poorly suited to automation. A common approach to the underlying data would allow those requirements to become more precise and easier to implement.

Policy Recommendations

DOE should treat the RFI and implementation process as an opportunity to establish the foundation for a durable hardware-transparency ecosystem. In doing so, we recommend that the agencies take the following actions, guided by four principles grounded in our earlier analysis.

Actions:

1. **The Department of Energy should leverage convening authority from trusted partners with experience doing this kind of work to convene an open, multistakeholder process with the goal of establishing a common vision and shared definition for HBOM.** The process should begin with specific use cases and a proposed core: reusable information about physical components, their relationships, and provenance. It should also define the boundaries between HBOM data and linked risk evaluations, functional characteristics, and operational information, while establishing realistic expectations for initial implementation.
2. **The Department of Energy, in implementing the requirements for EO 14421, should build confidentiality and purpose-specific disclosure into them.** DOE should define the information or assurance needed for particular decisions and facilitate industry exploration of technical and institutional disclosure models.
3. **The White House should coordinate across the Federal Government to ensure HBOM initiatives are implemented iteratively.** White House components should align relevant concepts and data requirements with other agencies and sectors, use pilots to test feasibility, and allow requirements to mature as tools and implementation practices improve.

To guide these activities, federal agencies should rely on the following principles:

- a. **Treat component coverage, provenance data, and data assurance as separate concepts.** Agencies should seek appropriate component coverage while applying risk-based requirements for how deeply particular components must be traced and how strongly the resulting assertions must be supported.
- b. **Require HBOM assertions to communicate their scope and limitations.** These assertions should distinguish “not present” from “not known” and “known but not disclosed,” without relying on a single completeness label that conflates component coverage with provenance depth.
- c. **Prioritize interoperability and reuse of existing capabilities.** Agencies should build on current enterprise systems, data representations, standards, and tools. SBOMs, HBOMs, CBOMs, and other BOMs should be capable of linking to one another without being forced prematurely into a single artifact or schema.
- d. **Address configuration and lifecycle change.** HBOM practices should account for production substitutions, different configurations sold under the same model number, maintenance and refurbishment, and changes in the availability or quality of provenance information.

The Executive Order places component-level provenance near the center of bulk-power supply-chain security. **DOE now has an opportunity to develop the definitions and information practices needed to make that objective workable.** An effective HBOM framework will not answer every supply-chain risk question. It will provide reusable, interoperable information that allows government and industry to ask those questions more precisely and answer them with better evidence.

About the Authors

Dr. Allan Friedman is a Senior Adjunct Technical Advisor at the Institute for Security and Technology and a cybersecurity policy expert whose work has helped shape modern approaches to software supply chain transparency. During more than a decade in federal service at NTIA and CISA, he led efforts to advance Software Bills of Materials (SBOMs) and related cybersecurity initiatives. His current work focuses on transparency across software, hardware, and AI supply chains, and he advises industry on related risk management practices as Technologist-in-Residence at TPO.group.

Nicholas Leiserson is the President of the Center for Advancing Cybersecurity at the Institute for Security and Technology (IST), where he previously served as the Senior Vice President for Policy. A legislative strategist and technologist, he has spent 15 years addressing cybersecurity risk and resilience and managing multidisciplinary teams of senior professionals at the White House and on Capitol Hill.

This policy memo is published in accordance with the Institute for Security and Technology's [Intellectual Independence Policy](#). The authors are solely responsible for the analysis and recommendations contained therein. The Institute for Security and Technology and its supporters do not determine, nor do they necessarily endorse or advocate for, any conclusions put forth in the comments.

Endnotes

- 1 This paper was drafted in response to DOE's Request for Information, "Securing the United States Bulk-Power System," Docket No. DOE-HQ-2026-1123.
- 2 See U.S. Department of Justice, "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide," March 24, 2022, <https://www.justice.gov/archives/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical> (Describing the Dragonfly/Havex campaign, which inserted malware into legitimate industrial-control software updates and infected thousands of devices, including systems used by power and energy companies); Laila Kearney et al., "'Ghost machine': Rogue communication devices found in Chinese inverters," Reuters, May 14, 2025, <https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/> (Reporting undocumented communications components in some Chinese-made inverters and the remote disabling from China of some inverters sold in the United States and elsewhere during a commercial dispute); Laila Kearney, "U.S. probe finds no evidence of spyware in Chinese power inverters," Reuters, February 10, 2026, <https://www.reuters.com/sustainability/climate-energy/us-probe-finds-no-evidence-spyware-chinese-power-inverters-2026-02-10/>, (Reporting that DOE found no definitive evidence of intentionally malicious wireless functionality in the units examined, while identifying documentation discrepancies and emphasizing the risks associated with remote access).
- 3 Executive Order 14421, "Declaring a National Emergency to Secure the United States Bulk-Power System," 91 Fed. Reg. 55,995, August 31, 2026.