National Institute of BUILDING SCIENCES™

BIM Event Series:

Collaborative Digital Delivery in the Age of Information Privacy and Cybersecurity

Final Report

Version 1, April 4, 2023

nibs.org

Table of Contents

1. BIM 2022 Series Overview: People, Process, and Technology

The National Institute of Building Sciences (NIBS) held a three-part event series that convened a group of experts within the built environment to discuss the impacts of data and information security regulations on the advancement of project delivery and operations using Building Information Management (BIM).

There is an increasing desire and practical demand for more efficient and collaborative digital delivery; however, cybersecurity threats to the built environment stemming from cyberterrorism and security breaches pose a real challenge to innovation and technology adoption.

The goals of this series were:

- Explore the current state and challenges facing the industry
- Lay the groundwork for future exploration
- Provide data that identify and prioritize topics and action items the NIBS BIM Council can harness to improve the industry in the area of cybersecurity and data privacy for collaborative digital delivery

The series kicked off with a webinar on June 1, 2022 that explored the current state and challenges, followed by an in-person workshop in Washington, DC, on June 7, 2022, that engaged experts in a deep dive of related opportunities, risks, and wastes. The series concluded with a presentation at Building Innovation 2022 at the Mayflower Hotel in Washington, DC on September 27, 2022, that outlined the analysis and findings of the webinar and workshop.

The series was developed and hosted by the NIBS Building Information Management Council, and sponsored by BSI Group, Compass Datacenters, dRofus, Newforma, and Autodesk. This report is a summary of the findings of these events.

Participants and Organizations

This Event Series brought together over 50 participants representing 30 stakeholder organizations including:

- Allegion
- Amazon
- Autodesk
- British Standards Institute (BSI Group)
- Burns & McDonnell
- Centre for Digital Built Britain (CDBB)
- Chinook
- Compass Data Centers
- Connected Places Catapult
- Construction Progress Coalition (CPC)
- Department of State
- Department of Veterans Affairs
- DPR
- dRofus
- ESRI
- FHWA
- GSA
- HDR Inc.
- Hensel Phelps
- International Code Council (ICC)
- Iowa Department of Transportation
- McCarthy
- Microsoft
- Newforma
- NIBS
- Penn State University
- Prime AE Group
- Procore Technologies
- Sundt Construction
- Trimble
- University of Washington
- USACE
- WSP

Series Moderators

- Connor Christian, PE, Senior Product Manager, Procore Technologies
- Roger Grant, fBSI, Executive Director BIM, NIBS
- Brok Howard, Product Manager, dRofus
- Rachel Riopel, AIA, NCARB, Digital Practice Leader, HDR Inc.
- Nathan C. Wood, Executive Director, CPC

Series Key Contributors

- Lynn Burns, ISSM & FSO, HDR Engineering
- Johnny Fortune, (formerly) BIM Manager, PRIME AE Group
- Wanda Lenkewich, CEO, Chinook Systems Inc.
- Alexandra Luck, Fellow, the Institution of Civil Engineers
- Dr. Ivan Panushev, Principal Partner Solutions Architect for Engineering, Construction, and Real Estate, AWS
- Robert "Bobby" Prostko, Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer, Allegion
- Rahul Shah, Sector Development Director, BSI Group Inc.
- Dr. Carrie Sturts Dossick, P.E., Professor of Construction Management, Associate Dean of Research, College of Built Environments, University of Washington

Webinar Presenters

- Lynn Burns, ISSM & FSO, HDR Engineering
- Alexandra Luck, Fellow, the Institution of Civil Engineers
- Horatio McDowney, Information Technology Applications Project Specialist, U.S. General Services Administration
- Robert "Bobby" Prostko, Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer, Allegion
- Rahul Shah, Sector Development Director, BSI Group Inc.

Workshop Panelists

- Johnny Fortune, (formerly) BIM Manager, PRIME AE Group
- Wanda Lenkewich, CEO, Chinook Systems Inc.
- Dr. Ivan Panushev, Principal Partner Solutions Architect for Engineering, Construction, and Real Estate, AWS
- Dr. Carrie Sturts Dossick, P.E., Professor of Construction Management, Associate Dean of Research, College of Built Environments, University of Washington

Workshop Breakout Session Facilitators

- Alex Belkofer, VDC Director, McCarthy Building Companies
- Connor Christian, PE, Senior Product Manager, Procore Technologies
- Brok Howard, Product Manager, dRofus
- Rachel Riopel, AIA, NCARB, Digital Practice Leader, HDR Inc.
- Nathan C. Wood, Executive Director, CPC

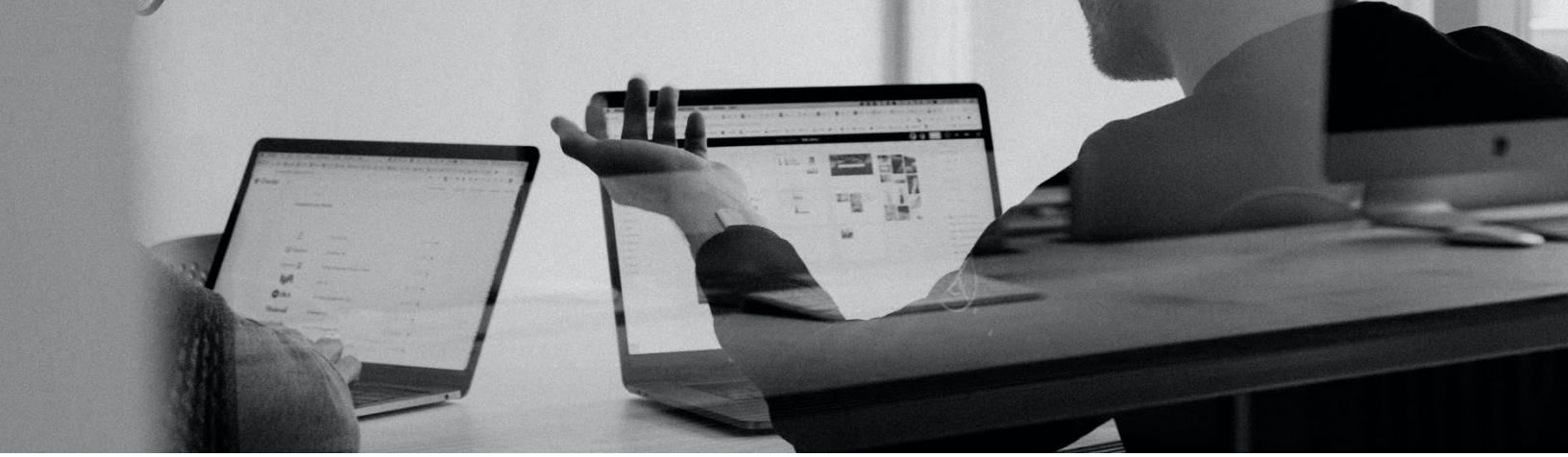
Building Innovation 2022 Wrap-up Session Presenters

- Rachel Riopel, AIA, NCARB, Digital Practice Leader, HDR Inc.
- Connor Christian, PE, Senior Product Manager, Procore Technologies
- Nathan C. Wood, Executive Director, CPC

NIBS BIM Council Board of Direction

NIBS would like to thank the BIM Council Board of Direction for their vision and diligent work in creating and delivering this series to address this important topic facing the industry:

- Chair: Rachel Riopel, AIA, NCARB, Digital Practice Leader, HDR Inc.
- Vice Chair (2022): Nancy Novak, Chief Innovation Officer, Compass Datacenters
- Vice Chair (2023): Mariangélica Carrasquillo Mangual, PMP, Chief, CAD/BIM Technology Center, U.S. Army Research and Development Center (ERDC) Information Technology Laboratory (ITL)
- Secretary: Alex Belkofer, CM-BIM, VDC Director, McCarthy Building Companies
- Industry Advisor: Shawn Foster – Director, Business Development and Customer Success, Allegion
- Past Chair: Van Woods – BIM Program Manwaterager, USACE



2. Webinar Summary

Highlighting an increasing trend in the building industry towards collaboration and the evolving requirements related to information privacy and cybersecurity, webinar attendees learned about key impacts of the requirements to the collaborative digital delivery process, how technology has evolved in support of collaborative digital delivery, and specific areas impacted by the requirements. (Link to webinar recording available here.)

2.1 Construction is the Least Digitized Industry

Nathan Wood opened the BIM webinar with a history lesson, recounting the eras of technological innovation starting with:

- Industry 1.0 (1784-1870) – Machined parts, steam power, weaving loom
- Industry 2.0 (1870-1969) – Mass production, assembly line, electrification
- Industry 3.0 (1969-Today) – Automation, computer processing, data storage, robotics
- Industry 4.0 (Today-Tomorrow) – Digital networks, internet of things (IoT), artificial intelligence

The presentation underscored the root causes of the construction industry's historic challenges with innovation, while posing tactical opportunities to move the needle towards Industry 4.0.

According to a 2015 McKinsey Global Institute Digitization Index, the construction industry has been among the least digitized, ranking just above agriculture and hunting . Since then, construction technology has seen over $10 Billion in venture capital investment seeking to capitalize on all of the untapped data produced throughout the design, construction, and operations of project.

2.2 Data Governance

With digitization, comes the need for data governance. Robert "Bobby" Prostko, Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer, Allegion, said there are many things that need to be considered before data is shared. First, it is important to ask and know who owns the data?

Prostko combed through foundational legal issues with preliminary intellectual property, privacy, and cybersecurity triage questions. These include:

- Who owns or has rights to the designs and data? What about derivatives and reuse?
- Is personal data involved? If so, what privacy laws are applicable? Cross-border transfers?
- What cybersecurity framework, controls, and/or laws apply? Is the project/information/data classified? Does it pertain to critical infrastructure? Is it covered by a non-disclosure agreement?

Details like general personal data (i.e., anything that allows you to merely identify an individual such as names and phone numbers) need not be protected as sensitive data such as social security numbers. Data governance should be defined in well-developed data standards.

2.3 Inhibitors to the Adoption of New Standards

Once standards are developed, there is the need for broad adoption and implementation. The inhibitors to the adoption of new standards are attributed to a few things. The tools and processes must be updated, and stakeholders need to be trained.

Brok Howard, Product Manager, dRofus, said he has been focused on BIM and collaboration through BIM for most of his career. Understanding the perspective is critical. As an architect, Howard would be focused on clients. Now as a product manager, he is focused on customers.

"Those people haven't changed," he said. "What's changed is my perspective. A larger project team has shared goals and different players involved, and we're all collaborating. At the center of that is data." Various perspectives exist within the building industry (owner, designer, information technologist, etc.). The most reasonable solutions take into account all of these perspectives.

When it comes to the federal security process, Horatio McDowney, Information Technology Applications Project Specialist, U.S. General Services Administration, likened adoption to a Formula 1 Pit Stop. In other words, the AEC industry is improving at a much slower pace compared to other industries, and the pit stop speed and safety improvements over time illustrate the need for changes to more than just tools and technology. It also requires changes to rules, policies, evolving racing strategies, staffing, resourcing, priorities on safety, and other issues. Summarily, a holistic approach could provide the AEC industry the same significant efficiency improvements as seen in the racing industry. For example, FedRAMP is the Federal Risk and Authorization Management Program which is designed to ensure security for cloud services for the federal government. The process to be FedRAMP compliant once was quite long (12 to 24 months), now it is 6 to 12 months. "AEC would like to speed up the federal security process," he said. "Cloud security is a dangerous thing." McDowney said FedRAMP places emphasis on security and protection of federal information and reduces duplicative efforts, inconsistencies, and cost inefficiencies.

Summarily, any solution to enabling collaboration yet remaining secure requires a holistic approach.

2.4 Driving Work Collaboration

A holistic approach requires solving both collaboration and security needs without comprising either. In the United Kingdom, making information more readily available and widely sharing it is a big driver toward collaborative work.

Alexandra Luck, Fellow, the Institution of Civil Engineers covered how the UK looks at the need for security. Traditionally, the UK looked at threats of espionage or terrorism. Today, it is seeing an increasing speed of threats, ranging from less-sophisticated hacker techniques to high-level criminal networks and terrorist organizations exploiting access.

Security governance requires top-level management buy-in, accountability, and responsibility.

"Gold-plated security need not be applied to absolutely everything," Luck said. "The amount of sensitive information is very limited," she said. "What is the information that could potentially compromise the safety, security, and the service the asset is to provide?"

Luck emphasized the need for a robust security approach that is not cost prohibitive for the short- and long-term. "Think about this in a holistic way," Luck said. "This isn't just about cybersecurity – it's about personnel, physical, and cybersecurity."

3. Workshop Summary

The second of the three-part BIM Event Series took place June 7, 2022. It involved a six-hour workshop in Washington, DC, that allowed the NIBS BIM Council leadership the opportunity to meet with industry stakeholders. The workshop was attended by 50 carefully chosen AECO industry-leading stakeholders to represent a wide array of perspectives while exploring four project typologies: *federal, data center, healthcare, and transportation*.

The workshop began with a brief recap of the preceding webinar followed by a panel discussion to prime the breakout sessions. Dr. Carrie Sturts-Dossick compared risks versus rewards from an Internet of Things perspective in relation to Facility Operations. Dossick highlighted the need for improving cross-departmental collaboration between Information Technologies and Facility Operations to ensure buildings can be both smart and secure. Johnny Fortune provided a design stakeholder perspective highlighting the challenges of professional service providers in understanding the highly technical and varying requirements, developing a systematic and systemic strategy, and implementing a compliance plan. Wanda Lenkewich emphasized the exponentially increasing vulnerabilities and exploitations impacting those in the industry. Dr. Ivan Panushev outlined many of the security features available in a cloud-based approach that generally exceed on-premise security. Nathan Wood led the transition from the panel discussion into the breakout sessions by framing the scope of the activities to consider opportunities, risks, and wastes while also pursuing balance between people, process, and technology.

The breakout sessions collectively revealed multiple opportunities, risks, and waste, which were common across the project typologies explored. From those commonalities, three key areas of capabilities, cost/benefits, and success/failures were discussed and led to three recommended analyses:

1. **Gap Analysis:** Assess the capability of organizations to implement new security requirements
2. **Cost/Benefit Analysis:** Compare the cost of implementation to the benefits of using new security requirements
3. **Root Cause Analysis:** Identify how current security practices fail and determine what will make them most likely to succeed

The workshop concluded with all breakout groups reconvening to provide a synopsis of the findings. The summary session highlighted the key opportunities, risks, and wastes identified by the groups. In general, the groups found that there are opportunities to secure and normalize data sharing, improve user experience in security integrations, and identify key performance indicators and value of a secure system. Identified risks include familiarity and compliance of users with security requirements, additional implementation costs, organizational capabilities to enforce security

standards, and excessive remote data collection that strains communications. Recognized wastes include the cost of changing or updating systems to meet changing requirements, time and effort in redundant validation, limited access to tools and technologies restricted by requirements, and data loss in transfer due to inconsistent data standards. Additional details of the workshop findings from the breakout sessions and the collective group are provided in the subsequent section.

4. Workshop Findings

The workshop addressed four project typologies in breakout sessions – *federal, data center, healthcare, and transportation* – with the general intent to explore cybersecurity and data privacy issues in their respective applications. The groups were pre-populated to ensure a cross-section of individuals with varying experiences and stakeholder perspectives. Contributors for each group are listed in the Acknowledgements section. Each group was prompted with a series of questions to help identify opportunities, risks, and waste associated with the session topic.

4.1 Common Opportunities, Risks, and Waste Across Project Typologies

Several opportunities, risks, and wastes were identified during the in-person workshop. While there were unique opportunities, risks, and waste across the four project typologies, common themes emerged across project types, including:

Opportunities:

- Secure data sharing and normalization between stakeholder systems (e.g.: state, local, federal)
- Removal of ambiguity in requirements that make compliance difficult to understand and achieve
- Improvement of the user experience around the integration of security
- Identify the value of a secure system; address waste associated with adoption of secure procedures, enable distributed teams to securely operate without requiring continuous internet connectivity
- Simplify tech stacks through better security protocols; and new funding opportunities (With recent funding, can security become a focus?).

Risks:

- Varied interpretation of requirements/policies, inconsistent data entry, lack of security controls with the potential to put information in the wrong hands
- Workers unfamiliar with a security-minded approach may resist change

- Workers who experience barriers or roadblocks to completing their work may intentionally or unintentionally begin to circumvent or weaken the security measures
- Difficulty maintaining security when operating without internet connection
- Vulnerability of backup systems.

Wastes:

- Requirements are improperly applied because they are highly technical and difficult to understand.
- Resources are often spent chasing security enhancements that are not part of security requirements.
- Data that is meant to be shared securely can be lost due to inconsistent transfer protocols.
- Processes can be inefficient due to security requirements limiting access to tools.
- Organizations often perform the same validation multiple times to meet different security requirements.
- Sunk Cost when changing to new security system
- Cost of time to update systems when new updates arrive (time for IT to implement, downtime of users)
- Export and import procedures take time vs. direct transfer.

4.2 Project Typology Specific Opportunities, Risks, and Waste

Type: Federal Project Facilitator: Rachel Riopel | HDR Inc.

Opportunities:

- Secure data sharing and normalization between stakeholder systems. (e.g.: state, local, federal)
- Improve user experience around the integration of security.
- Identify KPIs of a secure process.
- Seek new funding opportunities. (With recent funding, can security become a focus?)
- Identify the value of a secure system.
- Inform policymakers of collaborative digital delivery practices to develop more effective policies.
- Educate stakeholders on the implementation of requirements to reduce misinterpretation.
- Remove ambiguity in requirements that make compliance difficult to understand and achieve.

Risks:

- Providing access to information while also keeping it secure (What's the right balance?)
- Workers not familiar with security minded approach may resist change
- Impact of security requirements on the speed of delivery team members that lack sufficient technology or capability. Cost to implement a process that is in alignment with security requirements
- How capable are organizations of enforcing security standards?
- Organizations being potentially non-compliant with contract requirements
- Flowdown to vendors not being controlled or monitored
- Varied interpretation of requirements/policies

Wastes:

- Sunk Cost when changing to new secure systems
- What are the impacts to data completeness when security measures are applied?
- Organizations often perform the same validation multiple times to meet different security requirements
- Limited access (due to security requirements) to tools causing inefficient workflows
- Improve user experience around the integration of security
- Requirements, Standards, and Specifications for cybersecurity are in a state of flux causing re-learning from project to project

Type: Data Center Project Facilitator: Nathan Wood | Construction Progress Coalition

Opportunities:

- Identify the value of a secure system.
- Identify KPIs of a secure process.
- Measure waste associated with secure processes. (How wasteful is a secure process?)
- Secure data sharing and normalization between stakeholder systems. (eg: state, local, federal)
- Improve user experience around the integration of security.

Risks:

- Workers not familiar with security minded approach may resist change
- Cost to implement a process that is in alignment with security requirements
- Vulnerability of backup systems
- Typical fast-tracking of projects and schedule constraints leads to work arounds from secure processes and procedures

Wastes:

- Sunk Cost when changing to new security system
- Cost of time to update systems when new updates arrive (Time for IT to implement, Downtime of users)
- Data that is meant to be shared securely can be lost due to inconsistent data standards

Type: Healthcare Project Facilitator: Brok Howard | dRofus

Opportunities:

- Enable distributed teams to operate securely without requiring continuous Internet connectivity.
- Improve user experience around the integration of security.
- Secure data sharing and normalization between stakeholder systems. (eg: state, local, federal)
- Identify the value of a secure system.
- Simplify tech stacks through better security protocols.

Risks:

- Segregation of personal data
- What is the risk of connecting disparate systems?
- Use of operating systems and their compliance with requirements. (Is a system vulnerable when it fails? Are backups secure?)

Wastes:

- Export and Import procedures (Could secure direct transfer save money/time?)
- The unnecessary work performed when security measures are applied more broadly than is necessary

Type: Transportation Project Organizing Facilitator: Connor Christian | Procore
Substitute Facilitator: Alex Belkofer | McCarthy

Opportunities:

- Secure data sharing and normalization between stakeholder systems. (e.g.: state, local, federal)
- Improve user experience around the integration of security.

Risks:

- Inconsistent data entry
- Workers not familiar with security minded approach may resist change
- Security measures may be applied more broadly than is necessary
- Maintaining security when operating without Internet connection
- Providing access to information while also keeping it secure (What's the right balance?)
- A lot of remote data collection and difficult to secure the communications

Wastes:

- Data that is meant to be shared securely can be lost due to inconsistent data standards.
- Limited access (due to security requirements) to tools causing inefficient workflows
- Organizations often perform the same validation multiple times to meet different security requirements.
- Requirements are different from state to state.

5. Findings and Analysis at BI2022

The BIM Event Series concluded at the NIBS annual meeting, Building Innovation 2022, at the Mayflower Hotel in Washington, DC in September 2022.

Federal security is one of the chief components of the cybersecurity conversation.

Rachel Riopel, AIA, NCARB, Digital Practice Leader, HDR, noted a few great drivers of the conversation which included: the U.S. Department of Defense's controlled unclassified information (CUI) policy enacted March 2020; and the Cybersecurity Maturity Model Certification (CMMC) that will become a requirement for performance on federal contracts, starting in 2023.

"Prime contractors may be denied an award if a subcontractor/teammate does not meet the CMMC requirements," Riopel said.

"Digital transformation requires multiple parties to align," said Connor Christian, PE, Senior Product Manager, Procore Technologies.

5.1 The Root Causes of "Waste"

Nathan Wood, Executive Director, CPC, shared the eight categories of waste that exist within a Lean system: *defects, overproduction, waiting, non-utilized talent, transportation, inventory, motion, and extra processing*.

These eight categories define "what" the waste is. Understanding "why" they occur – the root causes – comes down to any combination of people, process, or technology.

The root causes of waste were identified as mostly process (56 percent), but also equally people and technology (each 22 percent).

Identified wastes include:

"What" - The Waste	"Why" - The Root Cause(s)
Defect	▪ Requirements are improperly applied ▪ They are difficult to understand ▪ They are highly technical ▪ They were written by a technical subject expert
Extra Processing	▪ The enhancements were not part of the security requirement ▪ They are difficult to interpret
Waiting	▪ Process inefficiency and user downtime ▪ Time required for IT to implement ▪ Limited access to collaboration tools ▪ Overbearing security requirement
Overproduction	▪ Same validation is performed multiple times ▪ Different security requirements ask for the same information, but not in the same format ▪ Security requirements are applied more broadly than necessary
Non-utilized talent	▪ Decreased productivity with new security system ▪ Not enough investment in training and troubleshooting
Transportation	▪ Time required to upload and download files between project delivery stakeholders ▪ Systems are not equipped to enable a single source of truth that is accessible to all stakeholders

5.2 The Road Ahead – Levers of Change

Three objectives were identified in the summary at the Building Innovation 2022 meeting. These include:

- **Assessing** the capability of organizations to implement new security requirements
- **Comparing** the total cost of implementation with the short- and long-term benefits of implementing new security requirements
- **Identifying** the root causes of security practice failures to determine what changes are necessary to succeed.

The recommended approaches are:

- **Gap Analysis**
- **Cost/Benefit Analysis,** and
- **Root Cause Analyses.**

Closing the session, Dr. Carrie Sturts Dossick, P.E., Professor of Construction Management, Associate Dean of Research, College of Built Environments, University of Washington, mentioned that there is a lot of talk around building cybersecurity cultures.

"It seems like a really technical problem, that we deal with firewalls," Dossick said. "We need to build a cybersecurity culture with a vocabulary and practices. It seems like a technical problem, but it's really about people and process."

6. Next Steps

Available technology has evolved but the AECO industry remains slow to adopt digitization. Cybersecurity and privacy threats are real and exponentially increasing. New data and process requirements are being implemented but this potentially slows technology adoption in the industry and creates a natural strain between innovation and security. Blanket requirements and implementations of security protocols are costly and difficult to apply. Basic questions often surface about who owns what data, when, and for how long, as well as which requirements actually apply.

This topic of advancing collaborative digital delivery in the age of information privacy and cybersecurity is one that raises concern amongst many representatives of the architecture, engineering, construction, and owner (AECO) industry. Security of project-related data is becoming a rallying point for industry-wide participation and engagement. There are many opportunities with the current challenge as well as risks to avoid and waste to eliminate. The series revealed opportunities to normalize the securing of data sharing across various stakeholder systems, improve user experience to guard against circumvention of the security measures, and develop KPIs of a secure process. It also highlighted the risks inherent in too costly a solution, untrained personnel, and organizational enforcing capabilities. Finally, it uncovered the wastes of lost data from inconsistent standards or the inability to access data, lost investments that cannot be recovered, and lost time in repeated validation processes.

Stakeholder education is a primary need across the entire industry for those developing, referencing, delivering, checking, and enforcing the data requirements. As further industry education and engagement is critical to innovative advancements, the logical next steps include developing educational content and hosting subsequent workshops. Policy makers and writers should be engaged to provide clear and achievable requirements. In accordance with the recommendations from the series, additional next steps include performing more detailed gap, cost/benefit, and root cause analyses during a follow-up event in 2023. The output of the next event should identify solution-based strategies that can be applied by various stakeholders across a spectrum of project types.

7. Breakout Session Acknowledgements

The information gathered from the breakout sessions and the details in this report would not have been possible without the meaningful contributions of those who participated. We wish to thank all who volunteered their time and expertise to this series of events.

Federal

Facilitator: Rachel Riopel | HDR Inc.
Contributors:

- Adam Matthews
- Andy Blackmore (Angel Dizon delegate)
- Charles Hardy
- David Spehar
- Donna Dennis
- Edmund Newman
- Jason Fairchild
- Keith Bryan
- Mariangelica Carasquillo-Mangual
- Max Blumenthal

Data Center

Facilitator: Nathan Wood | Construction Progress Coalition
Contributors:

- Bobby Prostko
- Nathan Wood
- Adeniyi Ol
- Brian Filkins
- Chris Johnson
- Hannu Lindberg
- James Hong, Senior Security Engagement Manager
- Jon Brownstein
- Nancy Novak
- Tara Anderson

Healthcare

Facilitator: Brok Howard | dRofus
Contributors:

- Chris Bober
- Dan Stapula
- Elisabeth Dupois
- Garret Jaco
- Paul Gregory
- Robin Harper
- Russ Manning
- Steve Hutsell
- Van Woods

Transportation

Facilitator (Organizing/Planning): Connor Christian | Procore
Facilitator (Event Substitute): Alex Belkofer | McCarthy
Contributors:

- Clay Starr
- Eric Cylwik
- Jaganath Mallela
- Jason Maynard
- Jennifer Steen
- John Messner
- Lynn Burns
- Shawn Foster

About NIBS

The National Institute of Building Sciences (NIBS) is an independent 501(c)(3) non-profit, non-governmental organization that supports advances in building science and technology. Established by the U.S. Congress in the Housing and Community Development Act of 1974, Public Law 93-383, Congress recognized the need for an organization to serve as an interface between government and the private sector – one that serves as a resource to those who plan, design, procure, construct, use, operate, maintain, renovate, and retire physical facilities. NIBS brings together experts from throughout the building industry, design, architecture, construction, and government. They lead conversations to ensure that buildings and communities remain safe, and work to seek consensus solutions to mutual problems of concern.

About the Building Information Management (BIM) Council

The Building Information Management (BIM) Council (formerly known as the buildingSMART alliance®) is a unique organization helping the North American real property industry become more efficient. The BIM Council leads in the creation of tools and standards that allow projects to be built digitally before they are built physically through the use of building information modeling. Their vision is to achieve a sustainable and efficient architecture, engineering, construction, owner and operator industry enabled with effective work processes based on collaboration, information technology and open standards. Their mission is to lead the development and deployment of broadly adopted national information standards and best practices for the built environment, with a focus on significantly improving project delivery and operational processes.

NIBS continues to develop open standards and guidance for all aspects of building information modeling, starting with the U.S. National BIM Program: The Foundation for Digital Transformation of Capital Facilities and Infrastructure. An implementation plan that outlines a strategy to rapidly expand standardization efforts, including expanded roles in partnerships with organizations worldwide, was released in September 2022.

For more information see:

- NIBS BIM Council
- U.S. National BIM Program