Webinar: Collaborative Digital Delivery in the Age of Information Privacy and Cybersecurity

JUN 1, 2022 | 1:30 PM – 3:00 PM ET
WELCOME AND SPONSOR INTRO

Meet the NIBS BIM Council and our Sponsors

Roger Grant, FbSI
Executive Director Building Information Management | National Institute of Building Sciences
THANK YOU TO OUR SPONSORS
MODERATORS

Rachel Riopel, AIA
Digital Practice Leader, HDR
Chair of NIBS BIM Council BOD

Brok Howard
Product Manager, dRofus

Connor Christian, PE
Product Manager, Procore Technologies

Nathan C. Wood
Executive Director, CPC
KEY CONTRIBUTORS

Rahul Shah
Sector Development Director, BSI Group Inc

Dr. Ivan Panushev
Principal Partner Solutions Architect for Engineering, Construction, and Real Estate, AWS

Johnny Fortune
BIM Manager, PRIME AE Group

Wanda Lenkewich
CEO, Chinook Systems Inc.
KEY CONTRIBUTORS

Lynn Burns
ISSM & FSO, HDR Inc.

Carrie Sturts Dossick, P.E.
Professor of Construction Management, Associate Dean of Research, College of Built Environments, UW

Robert “Bobby” Prostko
Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer, Allegion

Alexandria Luck
Fellow, the Institution of Civil Engineers
**NIBS BIM PROGRAM**

**NIBS**
(Board of Directors)

**U.S. National BIM Program**

**BIM Program Partners**
(Steering Committee)

**BIM Council**
(Board of Direction)

**NBP Workstreams**
- Owner Adoption
- Project Delivery Implementation
- Stakeholder Engagement
- Standards and Guidelines
- Education and Training
- Legal and Insurance

**U.S. National BIM Standard (NBIMS)**
- NBIMS-US Project Committee
- NBIMS-US Planning Committee
- NBIMS-US Content Workgroups
  - CORE BIM Workgroups
  - BIM Execution Planning
  - BIM Use Definitions
  - Information Standards
  - COBie
  - Additional under consideration

**U.S. National CAD Standard (NCS)**
- NCS Steering Committee
- Task Teams

[www.nibs.org/BIMC](http://www.nibs.org/BIMC)
PROGRAM VISION

To accelerate the digital transformation of the built asset industry to achieve optimal economic, environmental, and functional performance of our US built environment.

PROGRAM MISSION

To transform lifecycle information management practices by creating and advancing the consistent adoption of next-generation information management standards and practices to significantly improve the built environment delivery and operations processes.
LEARNING OBJECTIVES

WHAT ARE WE HERE TO LEARN?

Information on receiving Learning Units for today’s webinar will be emailed to you after the session.

Current Standards
Identify current standards and requirements related to information privacy and cybersecurity as it relates to the built environment.

Data Privacy
Recognize and state 1-2 key impacts of information privacy and cybersecurity requirements to the collaborative digital delivery process.

Technology Evolution
Explain how technology has evolved in support of collaborative digital delivery.

Impacts to Process
Identify 3 process areas impacted by requirements supporting information privacy and cybersecurity.
In-Session Polling Instructions

To engage everyone, we will be using a polling application called: Mentimeter!

Here’s how it works:

1. Scan the code to the right (using your phone)
2. Answer this first question as a trial run
3. Listen for cues to share your feedback throughout the presentation

The results from today’s surveys will be used in follow up work sessions.
Webinar: Collaborative Digital Delivery in the Age of Information Privacy and Cybersecurity

JUN 1, 2022 | 1:30 PM – 3:00 PM ET
AGENDA

01 WHY NOW?
02 TECHNOLOGY
03 PEOPLE
04 PROCESS
05 NATIONAL STANDARDS
06 WRAP
WHY NOW?
Stakeholders and the status quo

Rachel Riopel, AIA
Digital Practice Leader | HDR Inc.
BIM Council Chair
Stakeholder Perspectives

- Owners
- Designers
- Contractors
- Technology Partners
With Great Power Comes Great Responsibility

- Data Privacy Example – Cambridge Analytica + Facebook
- Cybersecurity Example – Colonial Pipeline Hack

Cambridge Analytica: how 50m Facebook records were hijacked

1. Approx. 320,000 US voters (‘seeders’) were paid $2-5 to take a detailed personality/political test that required them to log in with their Facebook account...

2. The app also collected data such as likes and personal information from the test-taker’s Facebook account...

3. The personality quiz results were paired with their Facebook data - such as likes - to seek out psychological patterns

4. Algorithms combined the data with other sources such as voter records to create a superior set of records (initially 2m people in 11 key states*), with hundreds of data points per person


Bloomberg

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

By William Turton and Kartikay Mehrotra
June 4, 2021, 1:58 PM MDT
WHY ARE WE HERE?
PREPARE TO ENGAGE

Inspire broader understanding of the impacts of security and data privacy on collaborative digital delivery by doing the following:

1. Establish a shared vocabulary
2. Identify key impacts to the delivery process
3. Understand implications in technology, people and process
4. Compile real world feedback to Inform the U.S. National BIM Program’s position on the matter
The topics we will address in today’s webinar are simply the beginning of what will be necessary to understand the impacts.

### Areas of Impact

**Why we should care?**

<table>
<thead>
<tr>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>How does this impact our relationships and ability to achieve quality delivery?</td>
<td>In what ways does this intersection impact our ability to achieve efficiency and productivity?</td>
<td>What are the boundaries?</td>
</tr>
</tbody>
</table>
TECHNOLOGY
Industry 4.0 Impacts on AEC Collaboration

Nathan Wood
Executive Director | Construction Progress Coalition
Welcome to Industry 4.0

- **Industry 1.0** (1800): The Industrial Revolution begins. Mechanization of manufacturing with the introduction of steam and water power.
- **Industry 2.0** (1900): Mass production assembly lines using electrical power.
- **Industry 3.0**: Automated production using electronics, programmable logic controllers (PLC), IT systems and robotics.
- **Industry 4.0**: The ‘Smart Factory.’ Autonomous decision making of cyber physical systems using machine learning and Big Data analysis. Interoperability through IoT and cloud technology.
The world’s most valuable resource

Data and the new rules of competition
Construction is Late to the Game.

The construction industry is among the least digitized.

McKinsey Global Institute industry digitization index; 2015 or latest available data

Relatively low
digitization

Relatively high
digitization

Digital leaders within relatively undigitized sectors

<table>
<thead>
<tr>
<th>Sector</th>
<th>Assets</th>
<th>Usage</th>
<th>Labor</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT²</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance and insurance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wholesale trade</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced manufacturing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oil and gas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Utilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemicals and pharmaceuticals</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic goods manufacturing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mining</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real estate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation and warehousing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail trade</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entertainment and recreation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal and local services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hospitality</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Construction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agriculture and hunting</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2Based on a set of metrics to assess digitization of assets (15 metrics), usage (11 metrics), and labor (8 metrics).
3Information and communications technology.

Sources: AppBrain; Bluewolf; Computer Economics; eMarketer; Gartner; IDC Research; LiveChat; US Bureau of Economic Analysis; US Bureau of Labor Statistics; US Census Bureau; McKinsey Global Institute analysis
Visualizing Construction’s #SharedPains

What does this say about our industry collaboration practices?

2014 Box.com File Exchange Metadata Analysis

- **Red Node**: Internal Company Data
- **Blue Node**: External Collaborator Data
- **Red Edge**: Connection from Internal
- **Blue Edge**: Connection from External
- **Edge Width**: Thicker edge represents more frequent connections between users

Software

Media & Entertainment

Construction

Manufacturing

Financial Services

June 1st, 2022
How is Industry 4.0 “Rewriting the rules” of design + construction?
Do we have the tools we need for Construction 4.0?

CDX provides a visual language for project teams to define their collaboration standards. Using:
TECHNOLOGY
Industry 4.0 Impacts on AEC Collaboration

Nathan Wood
Executive Director | Construction Progress Coalition
On your project, how many applications are used to share information or collaborate?
When prompted on a new website to accept cookies, what do you do??
INFORMATION AND DATA PRIVACY

Foundational Legal Issues for Digital Delivery

Robert Prostko
Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer, Allegion

June 1st, 2022
Foundational Legal Issues

Preliminary Intellectual Property, Privacy, and Cybersecurity Triage Questions

1. Who owns or has rights in the designs and data? Derivatives? Reuse?

2. Is personal data involved? If so, what privacy laws are applicable? Cross-border transfers?

3. What cybersecurity framework and controls, and/or laws apply? Is the project/information/data classified? Critical infrastructure? Covered by an NDA?
General Data Protection Regulation

- Data Subject Rights Requests
- Data Protection Impact Assessment
- Privacy-by-Design
  - 7 Foundational Principles by Ann Cavoukian, Ph.D.
    - Proactive not reactive; preventive not remedial
    - Privacy as the default setting
    - Privacy embedded into design
    - Full functionality – positive-sum, not zero-sum
    - End-to-end security – full lifecycle protection
    - Visibility and transparency – keep it open
    - Respect for user privacy – keep it user-centric
- Privacy-by-Default
# U.S. State Privacy Laws and Effective Dates

<table>
<thead>
<tr>
<th>State Privacy Law</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>California Consumer Privacy Act (CCPA)</td>
<td>January 1, 2020</td>
</tr>
<tr>
<td>California Consumer Privacy Rights Act (CPRA)</td>
<td>January 1, 2023</td>
</tr>
<tr>
<td>Colorado Privacy Act</td>
<td>July 1, 2023</td>
</tr>
<tr>
<td>Connecticut Data Privacy Act</td>
<td>July 1, 2023</td>
</tr>
<tr>
<td>Utah Consumer Privacy Act</td>
<td>December 31, 2023</td>
</tr>
<tr>
<td>Virginia Consumer Data Protection Act</td>
<td>January 1, 2023</td>
</tr>
</tbody>
</table>
Common Privacy Themes Have Emerged

- Notice
- Legal Basis
- Data Security
- Breach Notice
- Data Transfer

- Proportionality
- Minimization & Retention
- Accountability
- Data Subject Rights
- Privacy-by-Design
Cybersecurity Standards and Laws

Depending on the nature and type of information and data, there are several different standards to align to or requirements that are applicable:

- **NIST SP 800-171**
  (Protecting Classified Unclassified Information in Nonfederal Systems and Organizations)

- **DFARS 252.204-7012**
  (Safeguarding Covered Defense Information and Cyber Incident Reporting)

- **FedRAMP**
  (Cloud authorization program for use with U.S. government)

- **ISO 27001**
  Information Security Management System
Secure, Scalable, and Simple

To be a great ecosystem partner, you need to master all three

Secure
Scalable
Simple

Physical  Digital  Cyber
INFORMATION AND DATA PRIVACY
Foundational Legal Issues for Digital Delivery

Robert Prostko
Deputy General Counsel, Intellectual Property and Cybersecurity, and Chief Privacy Officer | Allegion
When prompted on a new website to accept cookies, what do you do??
MENTIMETER:
IMPACT OF REQUIREMENTS

Rate the impact the following will have on your organization.
Where perspective and motivation overlap

Brok Howard
Product Manager | dRofus
Collaborative Digital Delivery in the Age of Information
Privacy & Cybersecurity.

June 1st, 2022
Collaborative Digital Delivery in the Age of Information
Privacy & Cybersecurity.
Mentimeter: Impact of Requirements

Rate the impact the following will have on your organization.
What is the greatest risk to your organization's cybersecurity?
CUI TODAY
Working with Controlled Unclassified Information

Lynn Burns
ISSM & FSIO | HDR Inc.
Controlled Unclassified Information (CUI)

All Unclassified Government Information Requiring Protection due to Law or Policy

US Critical Infrastructure Sectors where CUI may be a requirement

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Executive Order 13556 -- Controlled Unclassified Information

The White House
Office of the Press Secretary
For Immediate Release
November 04, 2010

June 1st, 2022
Government CUI

Current Policies

Bureau of Reclamation SLE 02-01, 6 Mar 2015

Department of Treasury, Directive 80-08, 19 Oct 2017

Department of Commerce (DOC) OPBM-NP-18-001, 14 Aug 2019

**Department of Defense (DOD)** 5200.48, 6 March 2020

Environmental Protection Agency (EPA) CIO 2158.0, 8 Dec 2020

General Services Administration (GSA) 2103.2, 10 Apr 2021

US Geological Survey (USGS) 431.7, 21 May 2021

Nuclear Regulatory Commission (NRC) MD 12.6, 3 Dec 2021

Tennessee Valley Authority (TVA) CUI Policy, 31 Dec 2021

Department of Energy (DOE) O 471.7, 3 Feb 2022

Department of Transportation (DOT) Order 1650.5, 10 Feb 2022
Federal Requirements for CUI in Industry’s Hands

**Physical Protections**

- Document Marking Requirements: Banners, Paragraph Markings, Distribution Statements, Shipping Protection, Access Limitation, and Lockable Storage

**Digital Protections**

- 110 Cyber requirements: Policies, Procedures, Checklists, Inventories, Two-Factor Login, Encryption, Access Controls, and Audits
CUI in the Cloud - FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

DOD Cloud Computing Security Requirements Guide details protection requirements or DOD CUI protected by Cloud Service Providers.
The Next Step: Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification (CMMC) will become a requirement for performance on Federal contracts in 2023.

Certification will require all companies working with controlled unclassified information to pass a NIST 800-171 audit by an external organization.

Government contracting officers will verify certification prior to contract award.

Prime contractors may be denied an award if a subcontractor/teammate does not meet the CMMC requirements.
CUI TODAY

Working with Controlled Unclassified Information

Lynn Burns

ISSM & FSQ | HDR Inc.
What is the greatest risk to your organizations cybersecurity?
How relevant is the NIST 800-171/CMMC (110 security measures) to your current/future work?
HOW DO NEW STANDARDS AFFECT OUR WORKFLOWS?
What’s inhibiting our move to new standards?

1. Tools need to be updated
2. Processes need to be updated
3. Stakeholders need to be trained
How relevant is the NIST 800-171/CMMC (110 security measures) to your current/future work?
MENTIMETER: IMPACT ON DELIVERY

How likely are the following to negatively impact your ability to deliver digitally?
FEDRAMP & THE AEC

What is FedRAMP and why do we need it?

Horatio McDowney

IT Applications Project Specialist | U.S. General Services Administration
When You Are In a Race

- Early Years (First F1 1950)
- Dangerous
  - Refueling - banned in 2009
  - Pit lane directly adjacent to the track (cars moving at 180 mph)
- Limited Involvement
  - Two Mechanics
  - Now team of ~ 20 people
- Rough Tools
  - Using hammers to remove wheels
  - Today pneumatic wrenches (wheel guns)
- Long
  - Up to 60 seconds
  - Today ~ 2.5 seconds (3+ seconds slow)
AEC Would Like to Speed Up the Federal Security Process

FedRAMP designed to ensure security for cloud services for the federal government

- Long Process
  - Now 6 to 12 Months
- Dangerous
  - Security of Cloud
  - More Dangerous Now
- Limited Involvement
  - White House and NIST Standards
  - Agency Involvement
- Rough Tools
  - 15 to 20 Security Documents
  - Li-SaaS and Mi-SaaS Processes
What is FedRAMP?

FedRAMP is the Federal Risk and Authorization Management Program

- Cost-effective, risk-based approach for the adoption and use of **cloud services** by the federal government
- Emphasis on **security** and **protection** of federal information
- Reduces **duplicative** efforts, **inconsistencies**, and cost inefficiencies

---

**FISMA**

Federal Information Security Modernization Act (FISMA) requires agencies to protect federal information

**OMB Circular A-130**

Office of Management and Budget (OMB) states that when agencies implement FISMA, they must use National Institute of Standards and Technology (NIST) standards and guidelines

**FedRAMP Policy**

FedRAMP leverages National Institute of Standards and Technology (NIST) standards and guidelines to provide standardized security requirements for cloud services; a conformity assessment program; standardized authorization packages and contract language; and a repository for authorization packages
Who Is Involved in FedRAMP?

- **FedRAMP Program Management Office (PMO)**
  - The Joint Authorization Board (JAB) is the primary governance and decision-making body for FedRAMP. The JAB consists of the Chief Information Officers from the Department of Defense (DoD), the Department of Homeland Security (DHS), and the General Services Administration (GSA)

- **Cloud Service Providers (CSPs; vendors)**
  - CSPs only need to go through the FedRAMP Authorization process once for each Cloud Service Offering (CSO) and perform continuous monitoring

- **Third Party Assessment Organizations (3PAO)**
  - As independent third parties, they perform initial and periodic assessments of cloud systems based on federal security requirements
  - List on FedRAMP Marketplace

- **Agencies**
  - Agencies use FedRAMP’s standardized baselines to evaluate the security of cloud services.
  - Work with CSPs to review the security posture and authorize the CSO
What Is the Wait?

- Depends on Agency Buy-In
- Depends on Vendor
- Depends on Level

---

The Authorization Process

**01 Preparation**
- Readiness Assessment (Optional, but highly recommended)
  - RAR Development
  - FedRAMP PMO Review of RAR
  - Remediation (if needed)
  - FedRAMP Marketplace Designation – Ready

**02 Authorization**
- Full Security Assessment
  - Security Authorization Package (SSP, SAP, SAR, POA&M)*

**03 Continuous Monitoring**
- Post Authorization
  - Ongoing Continuous Monitoring Deliverables
  - Annual Assessment

**Pre-Authorization**
- Partnership Establishment
- Authorization Planning
- Kickoff Meeting
- FedRAMP Marketplace Designation – In Process

**Agency Authorization Process**
- Agency Review of Security Authorization Package
- SAR Debrief
- Remediation
- Agency Final Review
- Agency Issues ATO
- FedRAMP PMO Review
- Remediation (if needed)
- FedRAMP Marketplace Designation – Authorized

* The full security assessment may be prepared in advance of the authorization phase, or completed during the authorization phase. This is dependent on the agency’s review approach.
The Core: NIST Security Controls

**Controls span the following:** access, auditing (logs), pen testing, config, recovery/backup, authentication, incident response, maintenance, media, physical security, personnel security, sys communication, vulnerability scanning, code, boundary protection/keys

- **Li-SaaS - 37+ Controls**
  - Mostly attest and few document
- **Tailored (Low) Level - 125 Controls**
  - Attest and Document
- **Mi-SaaS (GSA Only) - 69+ Controls**
  - Mostly attest and more document
- **Moderate Level - 325 Controls**
  - Mostly Document and some attest
- **High Level - 421 Controls**
  - Document and some attest
What Is Produced Via the FedRAMP Process

- Completed about 35 Security Documents
- Authorization to Operate Issued
- Plan for Continued Monitoring Including
  - Reviews of all documentation
  - Inclusion of additional components or capabilities
  - Remediation of any findings
  - Tasks for agency to ensure secure usage
  - Tasks for renewal/reissuance of ATO
What You Can Do to Prepare

- **Educate Yourself and the CSP**
  - What is the CSO and what parts will be targeted for the initial ATO?
  - Get them a list of the controls to evaluate their application
  - If they don’t have a 3PAO make sure they know they need one

- **Get IT Involved Early**
  - If your IT team can’t understand it, your security team may struggle

- **Get Security Involved Early**
  - Requesting FedRAMP Package

- **Answer Questions (with Your IT and Security Team)**
  - Help teams understand what application does
    - Get solid description of the application from IT
  - How will access be granted into system? Volume of users? Environments?
  - What systems will be integrated? How? What types of data? (field level)
  - What types of users?
  - Who will be managing the application?
Watch Out for Common Dangers in the Pit

- **False Starts**
  - Other security accreditations (StateRAMP)

- **Stalling**
  - Not having the right people
  - Not having the FedRAMP Package
  - Not understanding what CSO (or parts of the CSO) are targeted for an already accredited offering
    - Always ask: “Is that feature FedRAMP approved?”

- **Needing a Tune Up**
  - CSP attempting to circumvent controls

- **Fires**
  - CSP targeting wrong Impact Level
Additional Resources

- FedRAMP Resources
  - FedRAMP Website
    - Templates for Process
  - Training
    - Subscribe
  - Baselines

- NIST Resources
  - Control Resources
    - Families

- GSA Resources
  - IT Security Resources (procedural guidance on authorization process for each security level)
What is FedRAMP and why do we need it?

Horatio McDowney
IT Applications Project Specialist | U.S. General Services Administration
MENTIMETER: IMPACT ON DELIVERY

How likely are the following to negatively impact your ability to deliver digitally?
What is your familiarity with ISO 19650?
ISO 19650 – PART 5
A security minded approach to information management

Rahul Shah
Sector Director | BSI Group Inc.
Published as an international standard in 2018 based on BS 1192 and PAS 1192, this standard supports the organization and digitization of information about buildings and civil engineering works through building information modelling (BIM).
INFORMATION MANAGEMENT – IN THE CONTEXT OF ORGANIZATIONAL MANAGEMENT

[Diagram showing the relationship between organizational management, relationship management, asset & project management, and information management.]

- Delivery phase (PIM)
  - e.g. ISO 19650
- Operational phase (AIM)
  - e.g. ISO 55000 & ISO 21500
  - e.g. ISO 44001
  - e.g. ISO 9001

[Source: ISO 19650, modified]

ISO/IEC 27001
Information Security
“SECURITY MINDED” PROJECT INFORMATION MANAGEMENT

ISO 19650 is separated into multiple (soon to be six) parts. Each impacts a range of stakeholders at different times in the asset lifecycle.

- **ISO 19650-1**
  - Concepts & Principles
  - Applies to all stakeholders in design, construction, & operations

- **ISO 19650-2**
  - Delivery Phase
  - Applies to designers, general contractors, trade contractors

- **ISO 19650-3**
  - Operational Phase
  - Applies to asset owners and operators

- **ISO 19650-5**
  - Security-minded Approach
  - Applies to all stakeholders in design, construction, & operations

- **[ISO 19650-4]**
  - (to be published in 2022)
  - Information Exchange

- **[ISO 19650-6]**
  - (TBD)
  - Health & safety

**Security-minded**

Understanding and routinely applying appropriate and proportionate measures [to achieve a] state of relative freedom from potential cause of an incident which may result in harm in any business situation so as to deter and/or disrupt deliberate, unwanted, hostile, malicious, fraudulent and criminal behaviours or activities.
**ISO 27001**

Information security management

Information security requirements for an **individual** organization

ISO 27001 demonstrates your commitment to managing information safely and securely for all operations in your organization

**ISO 19650 Part 5**

Security-minded approach to information management (BIM)

The adoption of security-minded, risk-based approach that can be applied across, as well as within multiple organizations

ISO 19650 part 5 demonstrates your adoption of a proportional security-minded information management using BIM throughout the lifecycle of an asset, where sensitive information is obtained, created, processed, and/or stored
IMPLEMENTING ISO 19650 PART 5 – SECURITY STRATEGY
(Ultimate accountability has to remain with the asset owner or project client)

Establishing governance, accountability and responsibility for the security-minded approach. The top management shall appoint an individual at top management level accountable for the security-minded approach.
IMPLEMENTING ISO 19650 PART 5 – SECURITY MANAGEMENT PLAN

- Ultimate accountability has to remain with the asset owner or project client.
- Enables the agreed mitigation measures set out in the security strategy to be implemented in a consistent and holistic manner.
ISO 19650 – PART 5
A security minded approach to information management

Rahul Shah
Sector Director | BSI Group Inc
What is your familiarity with ISO 19650?
NATIONAL STANDARDS

Requirements in practice: An international perspective

Alexandria Luck
Fellow | The Institution of Civil Engineers
WHAT HAS CHANGED?

Increased use, and reliance on digital and communication technologies

Increased collaborative working

Greater sharing of information (open data)
WHAT IS THE THREAT?
SECURITY GOVERNANCE

- Top management
- Accountability
- Responsibility
WHAT IS SENSITIVE?
Developing and maintaining a holistic approach

Information security
- Personnel security
- Physical Security
- Cyber Security

Your organization
Your supply chain
NATIONAL STANDARDS
Requirements in practice: An international perspective

Alexandria Luck
Fellow | The Institution of Civil Engineers
How does your organization approach security?
Digital Transformation....It’s Complicated.

In Reality, Digital Transformation Requires Multiple Parties to Align

Figure 2. What is really happening

HR's opportunity is to help close the gaps among technology, individuals, businesses, and society and governments.

Curve 1
Curve 2
Curve 3
Curve 4

Technology
Individuals
Businesses
Public policy

1970s 1980s 1990s 2000s 2010s Today

Rate of change

Building Information Management Council
Collaborative Digital Delivery in the Age of Information Privacy & Cybersecurity.
June 1st, 2022
WHAT’S NEXT?

To move forward together the conversation must continue. Here are the next steps for the National BIM Program:

- **Collaborative Digital Delivery and Security Workshop**
- **National BIM Program leadership convenes**
- **Building Innovation (September 2022)**
THANK YOU!

Share your feedback in the follow up survey.

June 1st, 2022

Collaborative Digital Delivery in the Age of Information
Privacy & Cybersecurity.