Framework Review
www.buildingcybersecurity.org
Our Mission

Establish and sustain frameworks developed by stakeholders across multiple sectors and administered by a non-profit organization offering market-driven options to promote cyber protections in controls and devices for enhanced cyber-physical security and safety in an increasingly smart world.

Our Vision

Building Cyber Security (BCS) will be the premier global administrator certifying operational technologies, processes, training, and recovery plans for safe, secure use of controls and devices.
Framework Goals & Requirements

CORE DESIGN PRINCIPLES

• Leverage existing technical standards to avoid duplication
• Ensure framework is modular, evolving, and consistent with technology and industry changes
• Includes all building technology (OT and IT that supports/interfaces with OT)

REQUIRED OUTCOMES

• Foster a cybersecurity culture in the building industry
• Alignment of cybersecurity risk into business risk
• Stakeholder have incentive to adopted (insurance coverage)

Deliverables

1. Risk framework (with value model)
2. Industry Standard Profile
3. Certification & labeling scheme
CRE Cyber Risk Include Both OT & IT

**OT**
- PHYSICAL SYSTEMS
  - HVAC
  - Lighting
  - Access Control
  - Parking
  - Video Surveillance

**IT**
- BUILDING TECHNOLOGY
  - Building Management
  - Building Automation
  - IOT/Sensors

- INFORMATION TECHNOLOGY
  - Property Management
  - Billing
  - Work Order System

Cyber-Physical Risk (OT)

Information Risk (IT)
<table>
<thead>
<tr>
<th>BCS Rating Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OT Zones</strong></td>
</tr>
<tr>
<td>Building Functional Areas (Standard Zones)</td>
</tr>
<tr>
<td>Bronze: 59/86</td>
</tr>
<tr>
<td>Silver: 81/86</td>
</tr>
<tr>
<td>Gold: 86/86</td>
</tr>
<tr>
<td>Platinum: 86/86</td>
</tr>
<tr>
<td>Health Safety Environmental Areas (Essential Zones)</td>
</tr>
<tr>
<td>Bronze: 64/90</td>
</tr>
<tr>
<td>Silver: 85/90</td>
</tr>
<tr>
<td>Gold: 90/90</td>
</tr>
<tr>
<td>Platinum: 90/90</td>
</tr>
<tr>
<td>Security Processes Maturity Level</td>
</tr>
<tr>
<td>Repeatable:</td>
</tr>
<tr>
<td>Repeatable:</td>
</tr>
<tr>
<td>Repeatable:</td>
</tr>
<tr>
<td>Improving:</td>
</tr>
<tr>
<td><strong>IT Zones</strong></td>
</tr>
<tr>
<td>CIS Controls</td>
</tr>
<tr>
<td>IG1: 58/156</td>
</tr>
<tr>
<td>IG2: 133/156</td>
</tr>
<tr>
<td>IG3: 156/156</td>
</tr>
<tr>
<td>IG3: 156/156</td>
</tr>
</tbody>
</table>

* Final BCS rating is based on the lowest score between OT and IT scoring.
The BCS Framework is Based on Existing Standards and Controls

Facility Cyber Security Risk

Cyber-Physical Risk (OT)

Information Risk (IT)

ISA/IEC 62443

ISA Secure

CIS Center for Internet Security

NIST Cybersecurity Framework

ISO 270001

International Society of Automation

BRONZE
SILVER
GOLD
PLATINUM
BCS Assessment Prerequisites

- Established OT/IT security governance initiative
- Asset inventory
- Service provider inventory
- Risk assessment that includes OT/IT
- Partitioned assets into Zones and Conduits (segmentation)
Roles and Responsibilities

Delegates Responsibilities
Building Owner / Manager
- building automation suppliers
- control system suppliers
- building physical systems suppliers

Examples
- building owner
- building property managers

Standards
- ISA/IEC 62443-2-1 Owner
- ISA/IEC 62443-2-2 SPS
- ISA/IEC 62443-3-3 Systems

Certification/conformance
- BCS

Selects Products
Service Provider
- system integrators
- maintenance providers

Examples
- system integrators
- maintenance providers

Standards
- ISA/IEC 62443-2-4 Services
- ISA/IEC 62443-3-3 Systems

Certification/conformance
- IECEE

Provides Certified Services
Product / Technology Supplier
- building automation suppliers
- control system suppliers
- building physical systems suppliers

Standards
- ISA/IEC 62443-4-1 SDL
- ISA/IEC 62443-3-3 Systems
- ISA/IEC 62443-4-2 Components

Certification/conformance
- ISASecure
- IECCE

Examples
- building owner
- building property managers

Standards
- ISA/IEC 62443-2-1 Owner
- ISA/IEC 62443-2-2 SPS
- ISA/IEC 62443-3-3 Systems

Certification/conformance
- BCS
Roles and Responsibilities

Building Owner / Manager
- Delegates Responsibilities
- Provides Certified Services

Service Provider
- Selects Products
- Provides Certified Products

Product / Technology Supplier

Examples
- building automation suppliers
- control system suppliers
- building physical systems suppliers

Certification/conformance
- ISASecure
- IECEE

Examples
- building owner
- building property managers

Certification/conformance
- BCS

Examples
- system integrators
- maintenance providers

Certification/conformance
- BCS
- IECEE
OT Assessment Scheme

ISA/IEC 62443

BRONZE
SILVER
GOLD
PLATINUM
Why Use ISA/IEC 62443 for OT Security?

The consequences of a security breach are different for IT and OT

- IT consequences include information security risk
- OT consequences include information and physical risk, e.g.:
  - loss of life/health
  - damage to equipment under control
  - damage to the environment
  - loss of product integrity

ISA/IEC 62443 is risk based

- Security Level is based on risk assessment process
- Segmentation into Zones and Conduits

ISA/IEC 62443 is widely adopted

- International standard
- Used in multiple industries (e.g. processing, manufacturing, transportation, medical)
- Products certified to comply with 62443 are available (e.g. ISASecure)
OT Design Principles: CRE Profile

Develop an OT cybersecurity conformance scheme for Commercial Real Estate

- facilitate the understanding of security principles by building owners (and stakeholders)
- assist BCS assessors in understanding the BCS rating system
- first vertical segment is commercial real estate

Based on ISA/IEC 62443 Series, which is specifically aligned with OT

- Part 2-1 for Building Owner requirements (draft)
- Part 2-2 for Security protection ratings (draft)
- Part 3-2 for Cybersecurity risk assessment process
- Part 2-4 for Integration and Maintenance Service Providers
- Part 3-3 for System technical security requirements

Reference Models

- Independent Building Control Zones
- Integrated Building Automation System (IBAS)
- Internet of Things (IoT) Building Automation System (IoTBAS)
- As-built Zone and Conduit model can use elements from each
## Risk Assessment – Consequences and Impact

<table>
<thead>
<tr>
<th>Health/Safety/Environmental</th>
<th>Reputation/Brand</th>
<th>Financial</th>
<th>Productivity</th>
<th>Regulatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the disruption of business operations and outage impact?</td>
<td>How is reputation/brand affected and what is the reduction in customers and revenue due to loss of confidence?</td>
<td>What are the projected financial losses? Possible gain for adversary vs. loss to owner/operator.</td>
<td>What is the disruption of business operations and outage impact?</td>
<td>What is the cost of corrective action, fines, and legal judgement?</td>
</tr>
<tr>
<td>Score</td>
<td>Score</td>
<td>Score</td>
<td>Score</td>
<td>Score</td>
</tr>
<tr>
<td>Serious long term health implications/Occupant loss of life.</td>
<td>Reputation is irrevocably or Severely destroyed or damaged. Irreversible or Severe reduction in existing and potential customers</td>
<td>Irreversible or severe Financial Loss.</td>
<td>Disruption of Business Operations Resulting in Unprocessed sales and Clients.</td>
<td>Irreversible or Severe Corrective Action. Irreversible or Severe Fines or Legal Judgment.</td>
</tr>
<tr>
<td>Occupant discomfort.</td>
<td>Reputation is minimally affected; little or no effort or expense is required to recover. Minimal reduction in clients and candidates.</td>
<td>Minimal Financial Loss.</td>
<td>Disruption of Business Operations Resulting in Minimal Delay in Candidate and Client Processing.</td>
<td>Minimal Corrective action Costs. Minimal Fine or Legal Judgment.</td>
</tr>
</tbody>
</table>

**Essential Functions**

**Property Damage example**
Risk Assessment - Likelihood

- Risk = function of { Likelihood, Impact }
- Cybersecurity Likelihood = function of { P(Threat), P(Accessibility), P(Vulnerability) }
- Likelihood Assumptions
  - Threats are everywhere and have the means and motive to attack building control systems
    - Assume - P(Threat) = 1.0 (100%)
  - Building control systems have vulnerabilities, either known (unpatched), or unknown (zero-day)
    - Assume - P(Vulnerability) = 1.0 (100%)
  - Base overall likelihood on Accessibility to the Zone (Attack Surface)
- Cybersecurity risk = function of { P(Accessibility), Impact }

<table>
<thead>
<tr>
<th>Accessibility Level</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Low</td>
<td>Physical access only</td>
</tr>
<tr>
<td>2</td>
<td>Moderate</td>
<td>OT access (e.g. IBAS)</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
<td>IT access</td>
</tr>
<tr>
<td>4</td>
<td>Very High</td>
<td>Public access (e.g. Internet)</td>
</tr>
</tbody>
</table>
## Risk Assessment – Target Security Level

<table>
<thead>
<tr>
<th>Target Security Level</th>
<th>Accessibility Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 - Low</td>
</tr>
<tr>
<td>Impact Level 1</td>
<td>SL 1</td>
</tr>
<tr>
<td>Impact Level 2</td>
<td>SL 1</td>
</tr>
<tr>
<td>Impact Level 3</td>
<td>SL 2</td>
</tr>
<tr>
<td>Impact Level 4</td>
<td>SL 2</td>
</tr>
</tbody>
</table>
BCS Assessment Overview

**Preparation**
- Establish security program
- Inventory service providers
- Inventory assets including criticality
- Partition assets into zones and conduits
- Identify essential functions zones
- Perform risk assessment for each zone
  - Assess consequences
  - Assess likelihood (accessibility)
  - Determine Target Security Level

**Assessment**
- For each IT Zone
  - Assess IT security controls based on CIS Controls v8
- For each OT Zone
  - Assess owner security measure and maturity
  - Assess service provider security measures and maturity
  - Assess technical security measures based on Target Security Level

<table>
<thead>
<tr>
<th>IT Zones</th>
<th>Essential Function Zones</th>
<th>Standard Zones</th>
<th>Minimum Maturity Level</th>
<th>CIS Implementation Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>OT Zones</td>
<td>Bronze 62/90</td>
<td>Silver 62/90</td>
<td>Gold 62/90</td>
<td>Platinum 62/90</td>
</tr>
<tr>
<td></td>
<td>56/85</td>
<td>56/85</td>
<td>56/85</td>
<td>56/85</td>
</tr>
<tr>
<td></td>
<td>Repeatable</td>
<td>Repeatable</td>
<td>Repeatable</td>
<td>Improving</td>
</tr>
<tr>
<td>IG1</td>
<td>58/156</td>
<td>IG2 133/156</td>
<td>IG3 156/156</td>
<td>IG3 156/156</td>
</tr>
</tbody>
</table>
Building Functional Areas (Zones)

Fire Systems
• Fire Detection Systems (alarms)
• Fire Protection Systems (sprinklers)

HVAC Systems
• Ventilation, Chillers, Air Handling, Purification
• Air Quality, Health

People Transport Systems
• Elevators
• Escalators
• Moving walkways

Lighting Systems
• Standard lighting and shades
• Emergency lighting

Utility Systems
• Gas
• Water, Boilers, Filtration
• Electric (including Backup Generators, UPS, Solar, Wind)

Physical Access Systems
• Physical Security Control
• Video Surveillance
• People Count

A/V and Digital Signage
• Room Management, Music, Directories

Voice Communication Systems
• Standard
• Emergency

Voice Communications (wired & wireless)

Parking Systems
• Access
• EV Charging

Building Automation Systems

IT Systems
• Owner Network
• Property Management
Key Concept: Reference Model Security Zone

- **Security Zone**
  - set of assets with common security requirements
  - similar to network segmentation

- **Components**
  - Host device (e.g. Windows/Linux PC)
  - Software application (e.g. HMI)
  - Network device (e.g. switch, router)
  - Embedded device (e.g. PLC)
  - Zone access point (e.g. firewall)

- **Accessibility types (in order of increasing risk)**
  - Low (e.g. physical access, no network connection)
  - Moderate (e.g. physical access, network to/from OT zones)
  - High (e.g. physical access, network to/from IT zones)
  - Very High (e.g. physical access, network to/from Internet)

- **Security Levels**
  - allows selection of technical requirements based on risk

- **Maturity Levels**
  - maturity of policy, process, procedural requirements

- **Essential Functions**
  - Identify zones which have essential functions
Reference Zone Model Independent Building Control System

- Building or Campus
  - Building-related IT systems e.g., Property Management Systems, Maintenance, Data Analytics
- Building Control Systems (OT)
  - HVAC Systems
  - Fire Systems
  - People Transport Systems
  - Physical Security Systems
  - Lighting Systems
  - A/V and Digital Signage Systems
  - Voice Comm Systems
  - Parking Systems
  - Utility Systems
- External Access
- Scope of BCS Assessment
  - Enterprise Information Systems (IT)
Reference Zone Model Integrated Building Automation System (IBAS)

Scope of BCS Assessment

Building or Campus

Building-related IT systems
e.g., Property Management Systems, Maintenance, Data Analytics

Building Control Systems (OT)

Integrated Building Automation Systems (IBAS)

HVAC Systems
Fire Systems
People Transport Systems
Physical Security Systems
Lighting Systems
A/V and Digital Signage Systems
Voice Comm Systems
Parking Systems
Utility Systems

External Access
Reference Zone Model IIoT Building Automation System (IoTBAS)

Scope of BCS Assessment

Building or Campus

Cloud-based Enterprise Information Systems (IT)

Cloud Control Systems (OT)

IoT Building Automation Systems (IoTBAS)

On-premise (Edge)

HVAC Systems

Fire Systems

People Transport Systems

Physical Security Systems

Lighting Systems

A/V and Digital Signage Systems

Voice Comm Systems

Parking Systems

Utility Systems

Cloud (public, private, hybrid)

External Access

Building Cyber Security Preliminary
IT Assessment Scheme

BRONZE
SILVER
GOLD
PLATINUM
The Evolution of The CIS Controls™

- 2000: NSA/DoD Project
  - The Consensus Audit Guidelines (CSIS)
  - “The SANS Top 20” (the SANS Institute)
- 2021: The Critical Security Controls (CCS/CIS)
- The CIS Controls™
CIS Implementation Groups

**Crawl... (Bronze)....**

IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

**Walk... (Silver)....**

IG2 assists enterprises managing IT infrastructure with multiple departments and varied risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

**Run... (Gold)....**

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or minimize the impact of sophisticated attacks.

**Total Safeguards:** 156
# IT Assessment Scheme: CIS Controls v8

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
<th>Baseline</th>
<th>Plan</th>
<th>Do</th>
<th>Score</th>
<th>Achieve</th>
<th>Status</th>
<th>Score</th>
<th>Achieve</th>
<th>Status</th>
<th>Score</th>
<th>Achieve</th>
<th>Status</th>
<th>Score</th>
<th>Achieve</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Inventory and Control of Enterprise Assets</td>
<td>5</td>
<td>0</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
<td>5</td>
<td>0</td>
<td></td>
<td>5</td>
<td>0</td>
<td></td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>02</td>
<td>Inventory and Control of Software Assets</td>
<td>7</td>
<td>0</td>
<td></td>
<td></td>
<td>7</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>03</td>
<td>Data Protection</td>
<td>14</td>
<td>0</td>
<td></td>
<td></td>
<td>14</td>
<td></td>
<td>14</td>
<td>0</td>
<td></td>
<td>14</td>
<td>0</td>
<td></td>
<td>14</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>Secure Configuration of Enterprise Assets and Software</td>
<td>12</td>
<td>0</td>
<td></td>
<td></td>
<td>12</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>05</td>
<td>Account Management</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>06</td>
<td>Access Control Management</td>
<td>8</td>
<td>0</td>
<td></td>
<td></td>
<td>8</td>
<td></td>
<td>8</td>
<td>0</td>
<td></td>
<td>8</td>
<td>0</td>
<td></td>
<td>8</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>07</td>
<td>Continuous Vulnerability Management</td>
<td>7</td>
<td>0</td>
<td></td>
<td></td>
<td>7</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>08</td>
<td>Audit Log Management</td>
<td>12</td>
<td>0</td>
<td></td>
<td></td>
<td>12</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>09</td>
<td>Email and Web Browser Protections</td>
<td>7</td>
<td>0</td>
<td></td>
<td></td>
<td>7</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Malware Defenses</td>
<td>7</td>
<td>0</td>
<td></td>
<td></td>
<td>7</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Data Recovery</td>
<td>12</td>
<td>0</td>
<td></td>
<td></td>
<td>12</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
<td>12</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Network Infrastructure Management</td>
<td>5</td>
<td>0</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
<td>5</td>
<td>0</td>
<td></td>
<td>5</td>
<td>0</td>
<td></td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Network Monitoring and Defense</td>
<td>11</td>
<td>0</td>
<td></td>
<td></td>
<td>11</td>
<td></td>
<td>11</td>
<td>0</td>
<td></td>
<td>11</td>
<td>0</td>
<td></td>
<td>11</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Service Provider Management</td>
<td>7</td>
<td>0</td>
<td></td>
<td></td>
<td>7</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
<td>7</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Security Awareness and Skills Training</td>
<td>9</td>
<td>0</td>
<td></td>
<td></td>
<td>9</td>
<td></td>
<td>9</td>
<td>0</td>
<td></td>
<td>9</td>
<td>0</td>
<td></td>
<td>9</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Applications Software Security</td>
<td>14</td>
<td>0</td>
<td></td>
<td></td>
<td>14</td>
<td></td>
<td>14</td>
<td>0</td>
<td></td>
<td>14</td>
<td>0</td>
<td></td>
<td>14</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Incident Response Management</td>
<td>9</td>
<td>0</td>
<td></td>
<td></td>
<td>9</td>
<td></td>
<td>9</td>
<td>0</td>
<td></td>
<td>9</td>
<td>0</td>
<td></td>
<td>9</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Penetration Testing</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
<td>3</td>
<td>0</td>
<td></td>
<td>3</td>
<td>0</td>
<td></td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
## Security Measures (controls) by Function

<table>
<thead>
<tr>
<th></th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
<th>Platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>33</td>
<td>34</td>
<td>34</td>
<td>34</td>
</tr>
<tr>
<td>10</td>
<td>29</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>10</td>
<td>25</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>21</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>8</td>
<td>26</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td><strong>Building Systems (OT)</strong></td>
<td>64</td>
<td>85</td>
<td>90</td>
<td>90</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td>122</td>
<td>218</td>
<td>246</td>
<td>246</td>
</tr>
</tbody>
</table>
BCS Assessment ...Getting Started

- Establish OT/IT security governance initiative
- Asset inventory
- Service provider inventory
- Risk assessment that includes OT/IT
- Partitioned assets into Zones and Conduits (segmentation)
A Special Thanks to the “Breakfast Club”

- 600+ volunteered man hours
- 15+ Technical reviews (Pink Teams)

- CRE Owners – MetLife, CA Ventures, COPT
- System Integrators – McKenny’s
- Tech Suppliers – Otis, Eaton, Schneider Electric, JCI (Simplex Grinnell), Amazon
- NIST/MITRE
- TIA/UL
- CRE Consultants

Team
- Jason Christman
- Fred Gordy
- Steve Griffith
- Johan Nye
- Sebron Partridge
- Robert Portvliet
- Tony Sager
- E.J. von Schaumburg
Closing Remarks

Thank You

Questions?