Privacy Impact Assessment for Non-Ministry Public Bodies

Table of Contents

Use this privacy impact assessment (PIA) template if you work for or a service provider to a non-ministry public body in B.C. and are starting a new initiative or significantly changing an existing initiative.

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	ECU CCURE system upgrade
Organization:	Johnson Controls, Inc.
Branch or unit:	Vancouver
Your name and title:	Mr. Jan Groenewald
Your work phone:	604-202-4518
Your email:	jan.groenewald@jci.com
Initiative Lead name and title:	Jan Groenewald
Initiative Lead phone:	604-202-4518
Initiative Lead email:	jan.groenewald@jci.com
Privacy Officer:	Jan Groenewald
Privacy Officer phone:	604-202-4518
Privacy Officer email:	jan.groenewald@jci.com

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Related PIAs, if any:
None

1. What is the initiative?

Johnson Controls International (JCI) is a world leader in smart buildings, creating safe, healthy and sustainable spaces. JCI offers the world's largest portfolio of building technology, software and services. Supported by a team of more than 100,000 dedicated employees working across 150 countries, JCI is helping customers achieve their sustainability goals and power their mission.

JCI entered into a Project Agreement with Emily Carr University (ECU) to provide maintenance services in 2017, which includes provision and maintenance of an access control system for

cardholder access to physical doors and spaces on ECU's campus. This system has been in place for the last seven years utilising a P2000 platform. This is now being upgraded to a new system, the CCURE 9000 system.

In addition to cardholder access provisioning, JCI performs the following services across the ECU campus:

- Plant/Maintenance Services
- Roads, Grounds and Landscape Maintenance Services
- Help Desk Services
- Utility Management Services
- Environmental and Sustainability Services
- Security Services
- Custodial and Housekeeping Services

Overview of the P2000 system:

The current P2000 access control system in place is a propriety software platform developed, owned, and operated by JCI. The system is comprised of a server, which is located in the main ECU server room, mercury controller boards and two workstations located at the security desk. This system pulls student, staff, and faculty information from the ECU OneCard database (Colleague) to update card holder information and provide access to doors throughout the ECU campus. The data being pulled is stored locally on-site and is exclusively used by the access control system to provide authorization or deny access to a door when an individual swipes their card.

The current database information transfer is done via a third-party application called SwiftData (SwiftData is overseen by ECU and out of scope of this PIA). This integration enables the P2000 system to access and retrieve updates to user credentials. The data is transferred via a pinwheel application and data is only uploaded in one direction from the ECU OneCard database to the P2000 database. Information from the P2000 system does not transfer back to the ECU database.

The P2000 system is a closed system on a closed network (FM network) with no access to the internet. All JCI FM systems operate within the FM V-Lan and JCI has no login access on the ECU IT network. The two-networks (FM and ECU) share the same network infrastructure; however, they are separated by a virtual local area network (VLAN) which is administered by the ECU's IT department and supported by a third-party vendor, X-10.

There is no artificial intelligence (AI) utilized for or by this system.

Overview of the CCURE 9000 system:

The new CCURE 9000 system will replace the P2000 system. This application is part of the software house offerings owned by Tyco/JCI. CCURE 9000 is one of the industry's most powerful security management system providing 24/7 mission critical security and safety protection for people, buildings and assets. It provides a standard approach to physical access authorization throughout all buildings, regardless of age, layout or location that an individual can access on their workstation, laptop or mobile device. The native interfaces combined with the CCURE's Connected Partner Program helps deliver seamless integrations with over 300 third-party security and business technologies. While these technologies are available through the CCURE system, no additional third-party technology integrations are part of the CCURE system at ECU apart from SwiftData. There is no AI utilized for or by this system.

The database integration between the new CCURE 9000 application and the ECU OneCard database will be done using the same third-party integration: SwiftData. There is no change in the data being transferred by the pinwheel application or how the data is handled by JCI in the CCURE system.

Consistent with the P2000 system, the CCURE system is a closed system on a closed network (FM network) with no access to the internet. All networking connectivity is limited to the facility's FM network contained within a closed VPN and secured by Palo Alto Global Protect, a third-party contractor of JCI.

2. What is the scope of the PIA?

In 2023, ECU requested JCI to complete the PIA process to ensure data privacy and security controls provided by the P2000 and CCURE 9000 systems meet ECU, BC Government and FIPPA requirements. ECU determined that an approved PIA, including the resolution of all risk and mitigation controls, must be completed for the two systems prior to JCI's migration to the CCURE 9000 system.

The following activities are in scope:

- All access control data pulled from ECU systems to the P2000/CCURE 9000 systems.
- JCI's access to, use, disclosure, retention and destruction of the ECU access control data pulled specifically for the purposes of supporting authorization to physical doors / locations within ECU's campus.
- JCI's access to ECU's physical and network infrastructure for system maintenance and upgrades.
- JCI's approach to information privacy and security, including all relevant policies and procedures, certifications and requirements for FIPPA compliance as a service provider.

The following activities are out of scope:

- Apart from the access control data, any ECU or JCI information within the closed FM network.
- Assessment of the SwiftData third-party tool, which has been overseen and implemented by ECU.
- Any other activities undertaken by JCI that involve ECU Information / systems under the Project Agreement (additional PIAs forthcoming).

3. What are the data or information elements involved in your initiative?

JCI receives the information from ECU's Colleague via the SwiftData's Pinwheel Data Medium Exchange (DME) middleware platform, which is a data integration tool. Pinwheel is used to sync data between disparate systems and automate the provisioning and de-provisioning of access rights in an access control systems. The following data elements are captured in the P2000/CCURE 9000 database for staff, faculty, and students.

User Information

- First Name
- Middle Name
- Last Name

Badge Information

- Badge ID (pre-assigned unique IDs used to authenticate and track movement within a facility)

To note

- Badge ID is only required to track movement throughout the facility; first, middle and last name are not required.
- Access logs viewed by Garda security are provided access to all four data elements.
- The P2000/CCURE system logs additional elements:
    - At which card readers a badge was swiped
    - What cards were swiped at a specific card reader
    - What time and how many times
    - If the system provided access or not
- All actions are linked to the Badge ID. There are predetermined reports that are set up and the system users are only able to pull these specific reports. These reports are regularly requested by the ECU for any investigations.

The system is configured to retain only the latest version of the database table received from ECU – upon receipt of an updated table the old database table is wiped. As part of the

maintenance process, JCI retains one copy of the access control database table on the P2000 server as a critical backup. This critical backup is needed in the event of a complete system failure. This backup is encrypted and rewritten at each maintenance renewal, approximately every three months.

See Appendix B for a list of all data fields collected by the system or available to be collected by the system but not initiated by ECU at this time.

3.1 Did you list personal information in question 3?

Yes

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.Yes

4. How will you reduce the risk of unintentionally collecting personal information?

It is not possible to collect unintentional information as JCI only receives automated database changes as provided by ECU via SwiftData. The CCURE system will be set up the same way as P2000.

Given JCI only receives information provided by ECU, during this assessment it was flagged that ECU is responsible for reviewing the number of unique information elements transferred to the P2000/CCURE systems for access control purposes. In the past, ECU has provided varying amounts of personal information for a unique individual requiring access to ECU facilities, and a review of the requirements for inputting new individuals and submitting database table updates to JCI was underway at the time of writing. The intent of the review is to ensure the least amount of information that is necessary for access control purposes is provided in a consistent manner.

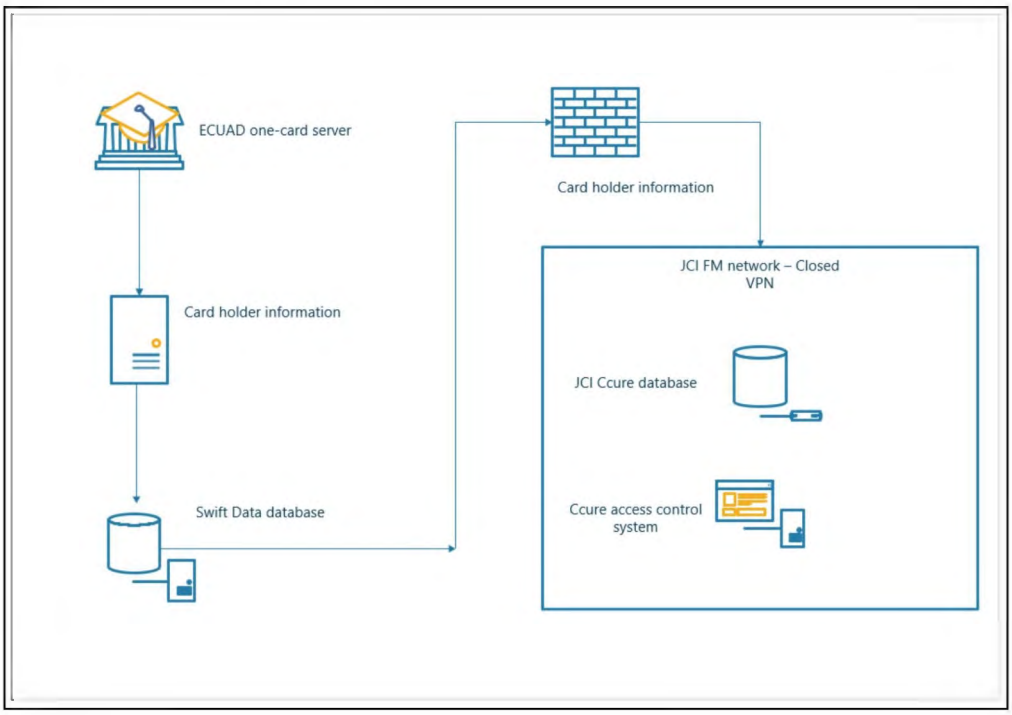
PART 2: COLLECTION, USE AND DISCLOSURE

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FOIPPA authority	Other legal authority
Step 1: ECU collects staff, student and faculty information to administer access accounts.	Collection	26(c)	
Step 2: ECU transfers the access account information via SwiftData to P2000/CCURE database; JCI stores the information on-site within ECU's server room.	Use	32(a)	
Step 3: JCI uses the information to administer access, to update the cardholder status, and to troubleshoot access issues.	Use	32(a); 32(c), 33(2)(t)	
Step 4: ECU facilities team uses the P2000/CCURE to add, change, or delete student, staff and faculty access cards.	Use	32(a)	
Step 4: JCI uses the information to respond to access control concerns (e.g., alarms; individual locked in room).	Use	32(a)	
Step 5: Data is stored on the JCI server located in ECU's main server room until deleted or overwritten.	Storage / Retention	30; 31	

Figure 1: JCI / ECU Data Flow Diagram



6. Collection Notice

A collection notice is not applicable as JCI is collecting the information from ECU, not directly from the individual. ECU's standard FIPPPA compliant collection notice considers the original collection of information by ECU and corresponding uses, including access control purposes.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

No personal information will be stored outside of Canada; all personal information will be stored locally on site at ECU.

8. Where are you storing the personal information involved in your initiative?

The stand-alone P2000 server (MS Server-2016) is located in the main server room at ECU, within the FM network which is a closed network with no access to the internet. Login access via VPN is password protected, with only a few select individuals from JCI having access (four individuals at the time of writing). Physical access to the server room is protected by the

security systems on site (access control, CCTV and intrusion system), and JCI operations oversee all site access and maintenance activity to the P2000/CCURE server. All physical and virtual access to the server by JCI is logged and monitored.

9. Does your initiative involve sensitive personal information?

No sensitive personal information is involved.

- If yes, go to question 10
- If no, go to Part 5

10. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

Type "yes" or "no" to indicate your response.

- If yes, go to Part 5
- If no, go to Part 4

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer. More help is available in the Guidance on Disclosures Outside of Canada.

Part 4 not applicable for this PIA. Please continue to Part 5.

11. Is the sensitive personal information stored by a service provider?

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12. **Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.**
13. **Does the contract you rely on include privacy-related terms?**
15. **What controls are in place to prevent unauthorized access to sensitive personal information?**
16. **Provide details about how you will track access to sensitive personal information.**
17. **Describe the privacy risks for disclosure outside of Canada.**

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

PART 5: SECURITY OF PERSONAL INFORMATION

18. Does your initiative involve digital tools, databases or information systems?

Yes, the P2000/CCURE systems involve a database and ECU's information systems.

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

Upon execution of the Project Agreement in 2017, a risk assessment was completed by JCI at service commencement and submitted to ECU. This included an assessment of all electronic systems and physical security. In addition, JCI completes a yearly audit of the P2000 system, and moving forward, will provide the results of the CCURE system's yearly audits to ECU for review and sign-off. Should any further auditing and /or controls be required upon ECU's review of the audit, JCI will complete the requested activities. Furthermore, upon transition from P2000 to CCURE 9000, an audit that considers physical and electronic security will be completed by JCI and provided to ECU.

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. What technical and physical security do you have in place to protect personal information?

The stand-alone P2000 server (MS Server-2016) is located in the main server room at ECU, within the FM network which is a closed network with no access to the internet. Physical access to the server room is protected by the security systems on site (access control, CCTV and intrusion system).

All access control database information that is (1) transferred from ECU's OneCard database and (2) logged when a user receives authorization to access a physical location on ECU campus, is stored only on the access control server and not transferred to any other location (physical or virtual) by JCI or its subcontractors. All information is encrypted in transit (TLS-1.2) and at rest using AES-256 encryption. Currently this is the P2000 server but will be migrated to the new CCURE server as part of the upgrade project. The system is configured to always retain only the latest version of the database table received from ECU. As part of the maintenance process JCI retains a copy of the access control database table on the P2000 server as a critical backup. This critical backup is needed in the event of a complete system failure. This backup is encrypted and rewritten at each maintenance renewal, approximately every three months.

On-site Access

Selected JCI security technicians are provided with secure login credentials to access the system manually on site. JCI operations staff oversee all site access and maintenance activity. Only four people currently have credentials to access this system (two JCI and two Tyco). Tyco is JCI's access controls systems installer and provides maintenance and demand service as needed. Tyco has entered into an agreement with JCI to provide these services and must provide similar privacy and security controls as JCI. All Tyco employees must sign a confidentiality agreement, engage in regular privacy training, and all access to the system is logged and audited by JCI.

Secure VPN Access

JCI employs, Palo Alto, a cybersecurity firm that provides the Global Protect VPN used to secure the JCI FM network. Palo Alto does not have direct access to any of the databases or servers, only the firewall and VPN tunnels. Palo Alto has entered into an agreement with JCI to provide these services and must provide similar privacy and security controls as JCI. All Palo Alto employees must sign a confidentiality agreement and engage in regular privacy training. All access by Palo Alto is logged and audited by JCI. Password requirements for the VPN and firewall are controlled by Palo Alto in line with industry standards, including prompted password changes, minimum password length and strength guidelines. Access is monitored via the Palo Alto's Global Protect application and the VPN account is automatically removed when an individual's access is revoked by JCI (in accordance with JCI's access control policies).

Secure Monitoring of Physical Access and Logs

JCI employs Garda, a provider of integrated security solutions, to provide on-site security guards to respond to access alarms and monitor physical safeguards throughout ECU's campus. Garda security guards have access to the active access log (view-only access) to monitor movements throughout campus and follow up on unauthorized activities. Garda security guards are only permitted to view the active log S.15 , which is physically situated in a secured workstation/room within ECU's campus. The access log is available 24/7 given S.15 S.15 is assigned to review and manage the system at all times (e.g., turn off doors, shut down building). In the case that no guard will be attending to the system, the door is secured to ensure no access is provided to S.15 / access log. To note, the guards do not log out of the access log system at any time and any actions taken by the guards to attend to activities flagged by the access log are logged by JCI via the P2000/CCURE systems. All guard monitoring functions are done withing security protocols stipulated in the Project Agreement (outside of this PIA's scope). All Garda employees completes a confidentiality pledge as part of their onboarding training and orientation or retraining, which strictly prohibits them from sharing any information from the access logs, and must engage in regular privacy training with JCI.

JCI Privacy Training

JCI staff must sign a confidentiality agreement and engage in privacy training, which is done via the JCI Global Cybersecurity Team training program. This training is repeated annually with periodic phishing and trojan penetration tests. If an individual does not pass a test additional refresh training is required.

Additional information about the CCURE and P2000 systems' cybersecurity controls is listed in Appendix C.

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Tracking is completed via the P2000/CCURE server login and events register. JCI does not log into the SQL database for any other reason other than database repairs. The databases is solely used electronically by the access control system. For tracking requests, a server log can be pulled by JCI and provided to ECU.

Strategy	
We only allow employees in certain roles access to information	Yes – Only authorised JCI technicians have access to the server for troubleshooting activities. All activities are logged and monitored. Garda employees only have viewing access to the active access logs; JCI logs Garda employee's use of the information to respond to access concerns via a separate log contained in the P2000/CCURE systems. Palo Alto and Tyco have no access to personal information. Authorized ECU employees receive logs from the system for review upon request (i.e. IT / Security / Facilities). A secure mechanism for transferring the logs is determined prior to transfer by both parties.
Employees that need standing or recurring access to personal information must be approved by executive lead	No recurring access required by JCI other than viewing access for Garda security guards, which is governed by the Project Agreement and confidentiality pledges undertaken by all Garda employees (privacy compliance overseen by JCI).

Strategy	
We use audit logs to see who accesses a file and when	Yes – all access by JCI technicians for troubleshooting activities is logged and reports are available to ECU at any time for review.
Describe any additional controls:	The database containing personal information of ECU staff, faculty and students is only accessible by the P2000/CCURE system or direct connection. Third party controls are in place via SwiftData for the transfer between ECU and P2000/CCURE, which is overseen by ECU's IT department.

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

JCI does not input any of the information into the system. This is managed by ECU. The information is only transferred and used by the system. JCI has no responsibility for the accuracy or completeness of the information.

Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

Correction to errors or omissions to personal information are completed by ECU and exported to the SQL database; JCI has no requirement for having a process in place to correct personal information in the database as it does not complete the original collection of it.

21.1 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Yes – if JCI receives a request to correct the personal information in its custody, it will document the request / annotate the record and follow up with ECU.

21.2 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

Yes – if JCI receives a request to correct the personal information in its custody, it will document the request / annotate the record and follow up with ECU, who oversees the notifications where necessary.

22. Does your initiative use personal information to make decisions that directly affect an individual?

- If yes, go to question 24
- If no, skip ahead to Part 7

No

23. Do you have an information schedule in place related to personal information used to make a decision?

No – JCI does not use the ECU supplied personal information to make decisions about an individual.

PART 7: PERSONAL INFORMATION BANKS

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

24. Will your initiative result in a personal information bank?

No – it will not result in a personal information bank.

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

25. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Possible Risk	Response	Risk Rating	Status/Timeframe
Risk 1: No standard FIPPA privacy schedule is attached to the 2017 Project Agreement between ECU and JCI. As a service provider to ECU, JCI must be bound by all FIPPA requirements and provide controls that meet or exceed ECU's privacy and information security standards. Without a FIPPA privacy schedule in place, this could lead to unauthorized access, use, disclosure of ECU information by JCI and/or its subcontractors. Furthermore, there are no binding requirements for breach reporting and remediation, which could lead to ECU information being comprised without proper breach reporting requirements undertaken by ECU.	ECU and JCI to work together to integrate the FIPPA privacy schedule into JCI's Operating Period Plans, which are reviewed and updated annually. Performance indicators and penalties must be attached to the privacy schedule / operating plan to ensure compliance by JCI.	HIGH	Status: complete
Risk 2: JCI engages in routine audits of its security controls and physical infrastructure hosted at ECU; however, audit reports were	JCI to work with ECU to develop a new audit report template that provides sufficient details about the testing,	HIGH	Status: audit report creation complete; migration audit to

Possible Risk	Response	Risk Rating	Status/Timeframe
not provided to ECU in the past. Give JCI's oversight of infrastructure on ECU's premises and its storage of personal information, ECU must be apprised of audit findings for additional review and scrutiny. Furthermore, audit reports provided by JCI to ECU to review during the PIA process did not provide sufficient information / details about controls tested and steps taken to remediate risk.	results, and remediation efforts taken by JCI's third-party auditor. ECU and JCI to establish a process to engage in a yearly review of the audit report, whereby ECU may request further testing by JCI after review of the results. JCI to complete an additional audit and provide results to ECU upon completion of the P2000 to CCURE system migration.		be completed August 2024 (post-migration activities).
Risk 3: ECU experienced significant difficulties and delays in receiving information during JCI's cybersecurity incident and privacy breach in 2023. ECU was unable to determine whether ECU information was implicated in the breach for weeks during the 2023 breach, which could have led to ECU's non-compliance with FIPPA breach reporting requirements. (JCI determined ECU information was not implicated at a later time.) To date, there has been no standardized cybersecurity response standard and plan in place between ECU and JCI to guide future scenarios of the like.	JCI to adopt ECU's cybersecurity incident reporting standard and cybersecurity incident response plan moving forward. ECU and JCI to jointly work to integrate both documents into JCI's Operating Period Plans, which are reviewed and updated annually. Performance indicators and penalties must be attached to the privacy schedule / operating plan to ensure compliance by JCI.	HIGH	Status: in progress JCI and ECU are in the process of finalizing the final document for integration with the Operation Period Plans in the Project Agreement. Expected to be completed by end of August 2024.

Possible Risk	Response	Risk Rating	Status/Timeframe
Risk 4: Given the joint nature of this PIA development, no authority has been appointed to own the document, and oversee yearly reviews and updates to the PIA. This could result in privacy and security risks going unidentified resulting in an insecure and non-compliant control environment moving forward.	JCI and ECU to determine which party will hold ownership of the PIA and its regular review. Given the nature of the partnership, both parties will need to be involved in the PIA review and updates.	HIGH	Status: work underway and will be completed by early August 2024. ECU's Executive is in the process of determining an approach that will be proposed to JCI in the near future.
Risk 5: As noted in the scope of work, this PIA is specific to the P2000/CCURE systems, and excludes all other services that are provided by JCI. No PIA has been conducted on the outstanding services to determine whether ECU staff, faculty and students' personal information is collected, used, and disclosed by JCI while supporting ECU for the services committed to in the Project Agreement. Given the lack of assessment, there is heightened risk of unauthorized access, collection, use and disclosure of personal information under ECU's custody and control.	ECU and JCI to complete a data mapping exercise to identify areas of JCI services whereby JCI has access to personal information under ECU's custody and control. JCI and ECU to determine an approach for completing outstanding PIAs and work towards drafting and sign-off in the 2024-2025 academic year.	HIGH	Status: no work completed to date. JCI and ECU to jointly map all remaining services that collect, use and disclose personal information and determine an approach to completing additional PIAs. Mapping and launch

Possible Risk	Response	Risk Rating	Status/Timeframe
			of new PIA expected to be completed by end of September 2024.
Risk 6: In addition to the standard information elements transferred to P2000 to date, there have been situations observed where additional elements have been transferred for random individuals. As outlined in Appendix B, the system allows for numerous pieces of information to be included about an individual. These columns should not be populated for ECU's instance; however, in the anomalies observed, it appears that the ECU representatives may have accidentally / unknowingly added more information than required on ECU's end for some individuals prior to transferring the database table to P2000. This could lead to the unauthorized use of personal information by JCI.	ECU to review internal SOP for populating database table and ensure that limited amount of personal information is submitted to the access control system. Given Badge ID is the only unique ID required for access control purposes, ECU to discuss the removal of first, middle and last name moving forward.	MEDIUM	Status: in progress ECU to confirm approach and updates to the database table by end of September 2024.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

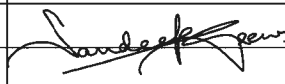
This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative	Adrian Tees		8 August 2024

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead	Sandeep Sidhu		7th Aug 2024
Program/Department Manager			
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate (if required)			

APPENDIX A: CCURE 9000 DATA PRIVACY SHEET

To note – Content taken from document without formatting for the purposes of the PIA.

Data Privacy Sheet - CCURE

Introduction to the Johnson Controls Global Privacy Office and Global Privacy Program

Johnson Controls has a Global Privacy Office and a Global Privacy Program, involved at the beginning and throughout the design and development of our processes, activities, products, services and solutions, in accordance with internationally accepted principles of Privacy by Design.

The Johnson Controls Global Privacy Office is led by the Chief Privacy Officer, and supported by Global Privacy Counsel, Global Privacy Professionals, Global Privacy Champions, analysts and support staff.

The Johnson Controls Privacy Program is designed with the most stringent global privacy and data protection laws in mind, including the General Data Protection Regulation (GDPR) of the European Union (EU), Brazil's Lei Geral de Proteção de Dados (LGPD), Singapore's Personal Data Protection Act (PDPA), and the California Consumer Privacy Act (CCPA).

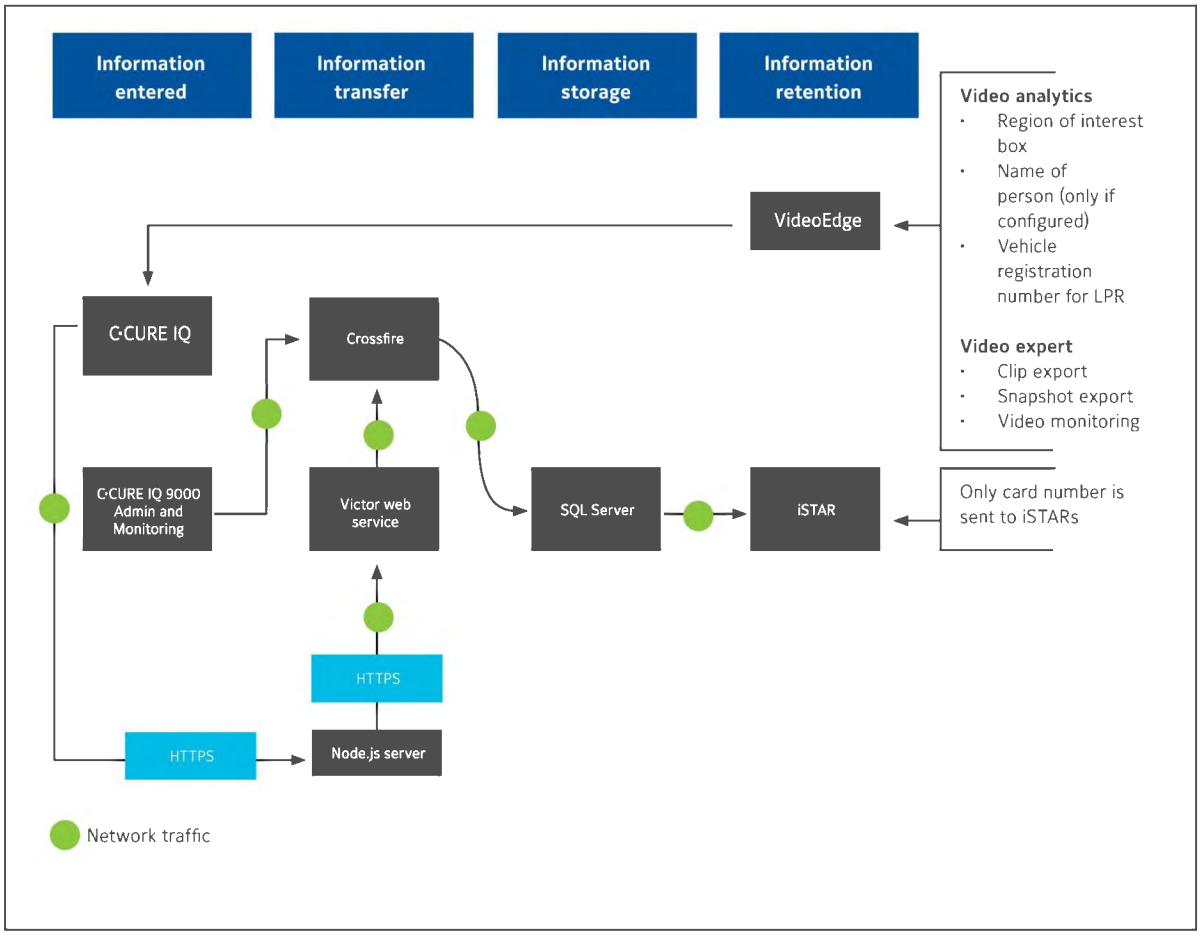
For more information on the Johnson Controls Global Privacy Office and Global Privacy Program, please visit www.johnsoncontrols.com/privacy.

Overview of C·CURE IQ

C·CURE IQ is the evolution of legacy C·CURE 9000 and victor VMS products. C·CURE IQ is built on a new, modern cloud-ready software platform, providing a standardized approach to security management. Customers are able to obtain real-time information and security event details, display dynamic views of doors, readers, inputs/outputs, controllers and video monitoring system activity in a single security operation center for better situational awareness and faster response times.

Information flow map for C·CURE IQ

Please see below the information flow map for C·CURE IQ, identifying where information is collected, stored and processed, and accessed and transferred. Please note that the specifics of this flow depend on the components chosen and deployed by the customer.



Personal data processing details of C·CURE IQ

See below for details on each category of personal data processed by C·CURE IQ, types of personal data within each category and the purpose of processing each type.

Types of Personal Data Processed	Purpose of Processing
• First name, middle name, last name • User login ID • User email ID • Phone number • License plate • Department • Personnel type (employee, visitor, contractor, etc.) • Credential • PIN • Address • Profile image • Badge in and badge out • Business unit • Work location	Access control

• Operator profiles and logins	

5. Data retention and deletion

Johnson Controls has a Global Records Management Program, which includes a Global Records Retention Policy and procedures. The purpose of our Global Records Management Program is to detail the responsibilities and working instructions necessary for the use, maintenance, retention or destruction of data, and to assign appropriate responsibilities to the right individuals.

When Johnson Controls processes personal data for our own purposes, the Johnson Controls Global Records Management Program applies to all records, on all media, and must be maintained in accordance with the Johnson Controls Records Retention Policy and Records Retention Schedule for the specific country and business in which the record has been stored.

The Global Records Management Program applies to all worldwide locations and legal entities controlled by Johnson Controls. Similarly, when Johnson Controls processes personal data on behalf of a customer, or when our products are operating on customer site, those offerings can be configured to meet customer data retention periods.

Data Privacy Sheet

6. Cross-border data transfers

This offering is designed to run on customer premises, solely within the control of the customer. In that situation, Johnson Controls will not process the personal data of this offering in any way. As a result, any cross-border data transfer issues and restrictions are a matter for our customer.

As a multinational organization, Johnson Controls has substantial experience in dealing with cross-border transfer issues and restrictions. When Johnson Controls processes personal data for our own purposes or on behalf of a customer, we utilize the following transfer mechanisms which can assist our customers:

Binding Corporate Rules (BCRs)	The Johnson Controls BCRs are designed to ensure an adequate level of protection of personal data no matter where in world it is processed by Johnson Controls. With respect to the European Union, the Johnson Controls BCRs have been specifically approved by the European Union Data Protection Authorities (DPAs) for transfer of EU personal data globally within Johnson Controls.
Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR)	The CBPR is a government-backed privacy certification which demonstrates that Johnson Controls complies with internationally recognized data privacy protections and is the framework approved for the transfer of personal data by Johnson Controls between participating APEC member economies: United States of America, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei, and Philippines.

Asia-Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP)	The PRP is a government-backed privacy certification that enables Johnson Controls to demonstrate to customers our accredited enterprise-wide Privacy Program, and to transfer data processed on behalf of our customers (including our cloud solutions) between the USA, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei, and the Philippines. Please see the PRP Directory and the Johnson Controls PRP TRUSTe validation page for more information.
EU Standard Contractual Clauses (SCCs)	Johnson Controls incorporates the EU's approved standard contractual clauses, also referred to as the Model Contract, into the Johnson Controls Data Protection Agreement located at www.johnsoncontrols.com/dpa to afford the contractual protection under the SCCs to our customers.
EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework	Johnson Controls was, and continues to be, certified under the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework. Although the Privacy Shield Framework has been invalidated by the Court of Justice of the European Union (CJEU), Johnson Controls intends to continue to maintain its certification for the foreseeable future, until a replacement framework is created.

Data Privacy Sheet

7. Privacy certifications

As explained above, this offering is designed to run on customer premises, solely within the control of the customer. In that situation, Johnson Controls will not process the personal data of this offering in any way. However, Johnson Controls has substantial experience with global privacy issues, and has achieved the below global privacy certifications which demonstrate our commitment to creating solutions which respect global fair information practices and Privacy by Design.

Asia-Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP)	The PRP is a government-backed privacy certification that enables Johnson Controls to demonstrate to customers our accredited enterprise-wide Privacy Program, and to transfer data processed on behalf of our customers (including our cloud solutions) between the USA, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei, and the Philippines. Please see the PRP Directory and the Johnson Controls PRP TRUSTe validation page for more information.

Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR)	The CBPR is a government-backed privacy certification which demonstrates that Johnson Controls complies with internationally recognized data privacy protections. Please see the CBPR Compliance Directory and the Johnson Controls CBPR TRUSTe validation page for more information.
TRUSTe Enterprise Seal	The Johnson Controls TRUSTe Privacy Certification Seal demonstrates our responsible data collection and processing practices consistent with regulatory expectations and external standards for privacy accountability. Please see the Johnson Controls TRUSTe validation page for more information.

Please note that this document is for customer guidance purposes only, is not legal advice and is subject to changes from time to time due to modifications of our solutions. Johnson Controls is not a law firm and does not provide legal advice. While Johnson Controls products and solutions are designed for use in compliance with applicable law, implementation and deployment of Johnson Controls products and solutions should be reviewed by appropriate customer advisors and stakeholders for such compliance.

APPENDIX B: ACCESS CONTROL DATA ELEMENTS

The following data elements are captured in the P2000/CCURE 9000 database for staff, faculty and students.

Currently Transferred to P2000/CCURE:

Personal Information

First Name

Middle Name

Last Name

Badge Information

Badge ID (pre-assigned unique IDs used to authenticate and track movement within a facility)

To note:

- Badge ID is only required to track movement throughout the facility; first, middle and last name are not required.
- Access logs viewed by Garda security are provided access to all four data elements.
- The P2000/CCURE system logs additional elements:
    - At which card readers was a badge swiped,
    - What cards were swiped at a specific card reader,
    - What time and how many times,
    - If the system provided access or not, etc.

  All actions are linked to the Badge ID. There are predetermined reports that are set up and the system users are only able to pull these specific reports. These reports are regularly requested by the ECU for any investigations.

Not Currently Transferred to P2000/CCURE:

Personal Information

ID

Phone

Extension

Email

Address Information

Suite

Address

City

State

Zip

Badge Informotion

BadgePublic

BadgePurpose

BadgeReason

BadgeDesign

BadgeDataStyle

BadgeStartDate

BadgeEndDate

BadgeDisable

BadgeExecPriv

BadgeTrace

BadgeOverride

BadgeFlagA

BadgeFlagB

BadgeFlagC

Access Information

AccessGrpoups

TimeZones

FacilityCode

Employment Information

Company

Department

Type

CardholderPublic

PortraitFile

SponsorID

Event and Security Information

EventPrivLevel

SecurityLevel

Miscellaneous

RecID

Result

RequestID

StartDate

EndDate

IssueLevel

PinCode

APPENDIX C: CCURE 9000 AND ISTAR CYBERSECURITY OVERVIEW

To note – Content taken from document without formatting for the purposes of the PIA.

C•CURE 9000 and iSTAR
Cybersecurity Overview

White Paper

Version 2.0
C•CURE 9000 v2.80
iSTAR v6.7
February 20202

Introduction

C•CURE 9000 provides peace of mind to our customers with a holistic cyber mind-set beginning at initial design concept, continues through product development, and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guaranty that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Executive summary

C•CURE 9000 and the iSTAR panels are versatile and secure Johnson Controls access control products. Adopted by government and critical infrastructure sites, financial, medical, and education institutes, C•CURE 9000 and the iSTAR panels have many certifications and security audits.

The encryption between C•CURE 9000 and the iSTAR Ultra and iSTAR Edge control panels has achieved FIPS 140-2 and FIPS 197 validation. When in FIPS-approved or "dark" mode, the iSTAR panels disable all access except direct communications from C•CURE 9000.

Both C•CURE 9000 and the iSTAR panels are developed under a Secure Development Life Cycle that includes secure coding techniques, strict source code control, regular vulnerability and penetration testing, and vulnerability management. When vulnerabilities are discovered after deployment, the cross-functional Cyber-Response team can provide a response the same day.

C•CURE 9000 and the iSTAR panel offer a secure platform that you can customize to meet the security policies of almost any installation and comes with a dedicated support team to address vulnerabilities and other security issues as they arise. This document serves to answer many of the frequently asked cybersecurity questions and identify some of the many security features available in C•CURE 9000 and the iSTAR panels. If questions or issues do arise, contact your Software House representative.

Our Product Security Program: Firmly established, always evolving.

Johnson Controls creates products and solutions in a culture focused on cyber resilience and we deploy with dedicated support. Our customers benefit from our proven approach:

- Consistent, organization-wide focus.
- Time-tested policies and practices.
- Global knowledge base.
- Support from design through deployment and beyond.
- Continuing investment to meet ever-evolving challenges and needs.

Structured methodology – Because disruption is not an option

Your facility's systems are crucial to continuing operations and maintaining profitability. Johnson Controls takes a holistic, structured approach to help you protect systems and sensitive data from the risk of a cyber-attack.

Disciplined governance. Our Product Security Team employs global governance to put cyber resilience at the forefront. We pursue and continually

improve a disciplined, policy-driven approach.

Expert-driven design. Engineering teams are trained in cybersecurity and in designing solutions that support compliance. Cybersecurity experts with certifications including, CISSP, CSSLP, CEH, and CCSP validate designs using up-to-the-minute best practices.

Security-infused development. We work to uncover, remediate and protect against concerns long before product release, through in-house testing that includes the integration of security tooling throughout the development lifecycle.

Knowledge-driven deployment. Through customer education, compliance assistance, security documentation, and our pragmatic approach, we help to facilitate more secure installation.

Lifecycle management. Cybersecurity continues to change, so our security approach goes beyond development and deployment to address tomorrow's concerns as they arise.

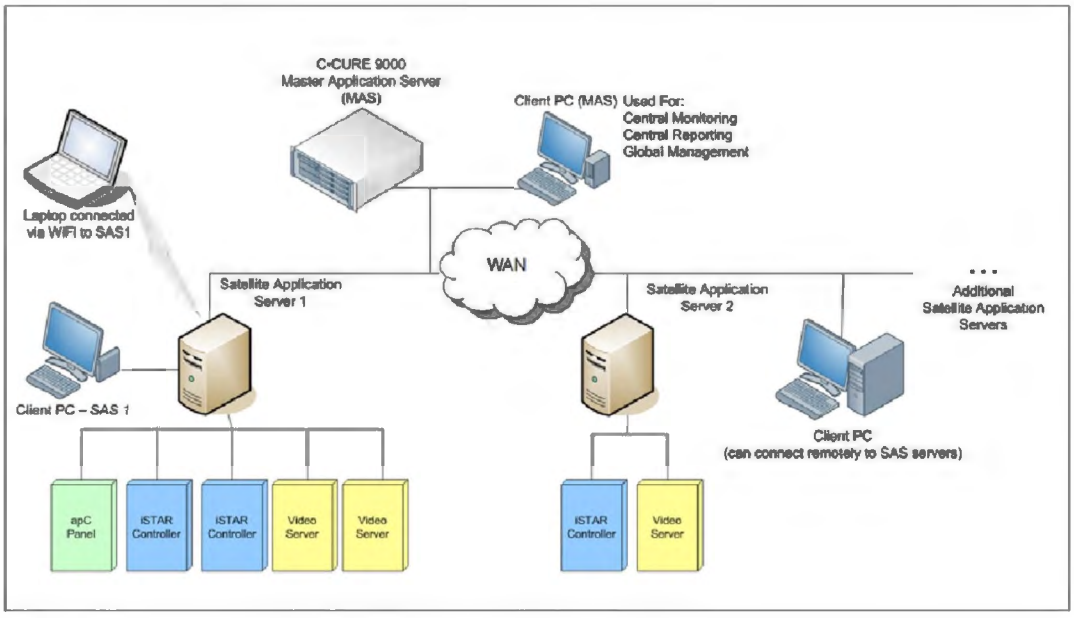
Rapid response. Our dedicated cybersecurity team emphasizes speed, transparency and professionalism. We monitor trends, assess new threats and provide guidance on handling vulnerabilities and reducing exposure.

Commitment to partnership. Johnson Controls is dedicated to sharing your responsibility for more secure systems. We support you through education, engagement and thought leadership for greater success in achieving your mission.

The C•CURE 9000 system

Architecture overview

Figure 1



C•CURE 9000 is a flexible, object-oriented security and event management system that features a variety of customizable interfaces for maintaining the system, and for monitoring the sites that you want to secure.

C•CURE 9000 provides extensive information management capability using Microsoft SQL Server and Microsoft .NET Framework V4.6.1. Its distributed client-server architecture is capable of supporting a large array of clients, controllers, and input devices, including various card readers and cameras.

C•CURE employs two thick clients. The Administration Station manages the customized C•CURE 9000 functions, objects, and views of the Monitoring Station. The Monitoring Station tracks events and status of devices, and can control manual actions such as locking and unlocking doors, depending on configuration and operator privileges.

The iSTAR panels are the hardware controllers that interface with access control card readers, locks, and other physical security hardware. They may be configured into clusters with a single master controller communicating to the iSTAR host and store a local version of the access control database so they can continue to operate during a network failure.

Enterprise architecture

C•CURE 9000 Enterprise Architecture is a licensable option that allows you to configure

multiple C•CURE 9000 servers to communicate with a Master Application Server (MAS). MAS provides a platform for global management of the Personnel, Video, and access security objects on two or more Satellite Application Servers (SAS) in an enterprise system.

MAS contains the global data that is used across every server, such as global Personnel records, global Clearances, and global Operators. The global data is synchronized to each SAS so that it can be used to implement enterprise-wide security. The MAS itself does not have any directly connected controllers or video servers, but it can be used to remotely monitor and manage controllers and video servers attached to SAS machines in the enterprise. The MAS provides the capability for Central Monitoring of the entire enterprise, using the C•CURE 9000 Monitoring Station application. You can view Events, Activities, and status of each SAS in the enterprise from a central Monitoring Station connected to the MAS. Alternatively, you can connect to a particular SAS to monitor that system and its connected hardware. In addition, the MAS provides a Central Reporting capability, because its database includes information about all objects that are replicated from the satellite servers.

Each Satellite Application Server contains database records for the video and access security hardware connected to it, in addition to local personnel, clearances, privileges, and other data. Each SAS synchronizes with the MAS so that SAS local data is replicated to the MAS for central management and monitoring.

All data is synchronized immediately when saved (or queued if a server is offline), except for Journal and Audit data, which is synchronized on a configurable schedule.

Note: Network latency and load on the MAS and SAS databases can affect synchronization performance.

Operator Privileges are used to provide system users with access to the information they need, and deny access to information they do not need or should not be able to view.

These capabilities let you deploy multiple C•CURE 9000 servers in an enterprise environment, solving scalability and wide area network issues and providing a platform for central monitoring, global management, and central reporting.

Microsoft Windows operating system

The licensed capabilities of C•CURE 9000 corresponds to the specific version of the Windows operating system it is installed upon. As the host environment, Windows10 provides the underlying foundation for configuring a secure C•CURE 9000 system. Tools such as Microsoft Security Configuration Manager, Security Compliance Manager and Windows domain policies can be used to optimize the security of the system. Additionally, the roles and responsibilities assigned to each C•CURE 9000 user is dependent on the specific Windows operator. This allows user credentials and access to the system to be controlled through Windows Active Directory.

Robustness

Backup/Restore

C•CURE 9000 uses three databases that you can back up at any time using the System Backup feature.

• The Core database is a core component of the management platform upon which C•CURE 9000 is built. It is the central repository for configuration details describing objects created, monitored, and maintained in C•CURE 9000.

• The Audit Log provides a history of changes to configurations managed by C•CURE 9000.

• The Activity Journal maintains a record of activity monitored by the system. Records in the Activity Journal provide a historical view of activity that has occurred within the system, statistical information on resource usage, and personnel and asset location information.

In the event of a system failure or corruption of the Core, Audit Log or Activity Journal database, you can restore one or more of these databases from a backup of the respective database.

The C•CURE 9000 Server Configuration Application Guide describes the details for performing system backup and restore.

User access to the System Backup feature is controlled through the user configuration.

Access control

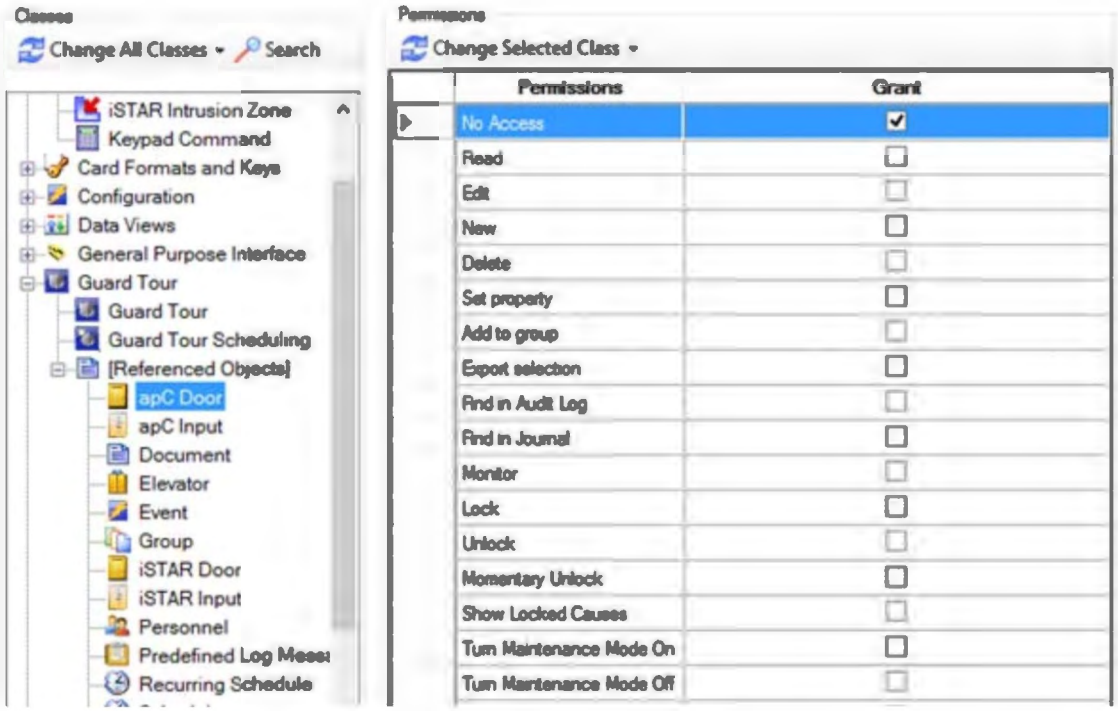
Authentication

C•CURE 9000 is designed for deployment in an Active Directory domain environment utilizing Windows Single Sign-On (SSO) to integrate login credentials with operator permissions. This provides a seamless user authentication and authorization process. Password rules and policies such as predefined number of login attempts, character11 length, combination of alpha numeric, and user-defined lockouts are managed by the local Microsoft Windows operating system or the domain controller. C•CURE 9000 does not store or have any visibility of the credentials.

Separation of responsibilities

C•CURE 9000 has highly configurable operator privilege functionality. Using the Privilege Editor feature, administrators can specify the objects, programs, reports, Personnel, events, and actions that Operators can view and use. The feature also allows for exceptions and bulk configuration.

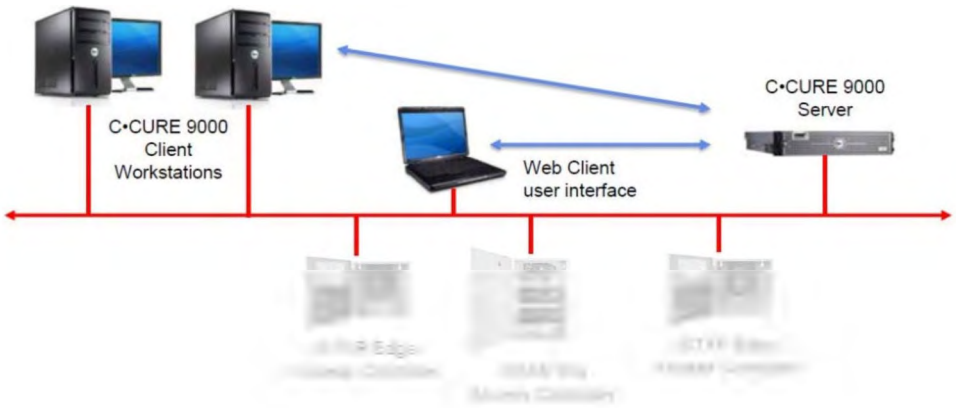
Figure 2



Communication protection

C•CURE 9000

Figure 3



Communication between the C•CURE 9000 server, iSTAR controller, database, or client devices uses the Crossfire service. By default, the CrossFire server uses AES-256

encryption that has been FIPS 197 validated.
(Line 2857): http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html13

iSTAR

In standard mode, the iSTAR Edge and iSTAR Ultra use TLS to communicate securely with the host and other cluster members. The encryption is FIPS 197 listed (AES 256).
Figure 4
In FIPS mode, the iSTAR will use TLS to authenticate the controller to the C•CURE 9000 host. The system may be set up to use a default certificate, or it may be set up to use a custom certificate provided by a third-party or auto-generated by the C•CURE 9000 host.
• Controller-Based Encryption Mode – C•CURE 9000 creates the Host and CA certificates at the C•CURE 9000 host computer and then directs the iSTAR encrypted controller to generate new public and private keys.
• Host Based Encryption Mode – C•CURE 9000 creates the Host, Controller, and CA certificates on the host computer and then downloads the Controller public key, the Controller private key and the CA certificate to the iSTAR controller. Host-Based Encryption allows the use of a certificate created by a third-party certificate authority.
The default asymmetric encryption is RSA 1024, but may be changed to ECC 571 at the cluster level. The symmetric key remains AES 256.
The iSTAR Edge and iSTAR Ultra are tested and listed for FIPS 140-2 level 2 for cryptographic modules:
• iSTAR Edge: FIPS 140-2 certificate #2309
• iSTAR Ultra: FIPS 140-2 certificate #2315
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm14

Also, in FIPS approved mode, the iSTAR controller disables all ports except those required for communication between the C•CURE 9000 host and other iSTARs in FIPS approved mode. It only accepts communication from the C•CURE 9000 host and the iSTARs in its cluster.
The iSTAR Ultra family supports TLS v1.2 only at minimum.

iSTAR operating system

The iSTAR Ultra family operating systems are Linux-based.
The embedded web server has been developed internally and may be turned off through the controller's setup screen.

Firmware updates

Firmware downloads are issued from the Monitoring Application or a separate utility

called ICU utilizing TCP port 1999. The panel continues to operate during the firmware download process. When the panel receives the proper check-sum, this signifies a successful download. The controller must reboot when a successful download is completed. After a successful reboot the server re-establishes communication issuing a fresh personnel and configuration download to the panel. If the panel does not receive the proper checksum then the panel continues to use the previously stored firmware.15

iSTAR database

The iSTAR downloads three specific data sets that allow it to operate and make access control decisions: cardholder data, configuration data, and firmware. When a controller is first placed online, the C•CURE 9000 iSTAR driver downloads all pertinent data to that panel. The fast personnel download and the configuration download take place at this time. The fast personnel download uses TCP port 2801. It creates a single file of all personnel data that have access privileges to any of the doors associated with the panel being placed online. All additional incremental system changes regarding cardholder or hardware configurations get downloaded in real-time. Major personnel changes implemented at the server cause the system to perform a fast personnel download to the panels that are affected.

By default the database on the iSTAR is encrypted with AES 256. However, if additional security is required, activating the CPNI mode on the iSTAR Ultra prevents the database from being stored in persistent memory.

ICU now redirects requests to edit any controller configuration setting such as IP address or Host IP, or downloading firmware back to the controller's local web page where editing can take place in a much more secure environment.

The web diagnostics user interface on the iSTAR provides the option to encrypt the main partition of the SD card (OS, access control FW, and customer DB). After the encryption process is finished, the panel boots up normally and continues operation without delay or configuration loss. And in C•CURE 9000 v2.80, you can display the Encrypted Status of each panel. Note that a unique key is used for encryption, so it is no longer be possible to change just the SD card on an iSTAR Ultra.

Enforced unique, strong password, for each controller, for the web diagnostics page. Web passwords must be changed upon initial controller boot up, and, you can change and manage this centrally through C•CURE 9000 v2.80.

Tamper detection

All iSTARs include tamper detection. If the enclosure has been opened an alarm is activated. The iSTAR Ultra includes an optional installation of a back tamper it case it is removed from the wall.

iSTAR Ultra and iSTAR Edge have been FIPS 140-2 approved to provide physical protection of the encryption module. This includes the metal enclosure, physical tamper,

preventing visibility, and using tamper evident labels.16

Security approvals and certifications

FISMA

You can configure the C•CURE 9000 system to support the controls necessary for overall FISMA compliance. These controls include:

- Authenticated system access.
- Account login/logout management.
- Role-based separation of capabilities, permissions, and privileges.
- System event and configuration change auditing, alerting, and management.
- Restriction of ports, protocols, and services to only those required to support C•CURE 9000 functionality.
- Encrypted communications.

FICAM FIPS-201 certified/GSA approved products lists

The Software House C●CURE 9000 has been tested and certified as an end-to-end physical access control system with high assurance readers and validation software. The system has been tested and approved as a fully compliant FICAM Solution by the U.S. General Services Administration. The approval means that the C•CURE 9000, high assurance readers and validation software meet the rigorous testing requirements and comply with the FICAM roadmap and the realignment of the GSA's Approved Product List (APL). The system was subjected to numerous tests to ensure that the system is not prone to denial of service, credential spoofing, or other types of unauthorized access that could compromise the security of the system. C•CURE 9000 provides a solution for HSPD-12 / FIPS-201 and 800-116 compliance for smart card credentials, along with support for PIV-I, PIV-C, TWIC and the DOD CAC credential using authentication software with its Server-based Certificate Verification Protocol (SCVP) client.17

FIPS 197

C•CURE 9000 and the iSTAR Controllers have been certified by the NIST CMVP as meeting the requirements of FIPS 197 AES encryption algorithm standard.

FIPS 140-2

The C•CURE 9000 iSTAR Edge and Ultra controller models have been certified by the NIST CMVP as meeting the requirements of FIPS 140-2 Level 2.18

APPENDIX – Resources and references

Johnson Controls documents

The following documents are available at https://www.johnsoncontrols.com/cyber-solutions

- C•CURE 9000/iSTAR Port Assignments
- C•CURE 9000/iSTAR FISMA-Ready Compliance Guide
- C•CURE 9000 v2.80/iSTAR NERC-CIP v6 Compliance Guide

Laws and regulations

- Federal Information Security Management Act of 2002
- Federal Information System Modernization Act of 2014
- Consolidated Appropriations Act of 2005, Section 522.
- USA PATRIOT Act (P.L. 107-56), October 2001.

OMB circulars

- OMB Circular A-130, Management of Federal Information Resources, November 2000.
- OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June, 2006.

FIPS publications

- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems

NIST publications

- NIST 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST 800-30, Risk Management Guide for Information Technology Systems
- NIST 800-34, Contingency Planning Guide for Information Technology Systems19
- NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST 800-53 Rev3, Recommended Security Controls for Federal Information

Systems and Organizations
• NIST 800-53A Rev1, Guide for Assessing the Security Controls in Federal Information System and Organizations
• NIST 800-60 Rev1, Guide for Mapping Types of Information and Information Systems to Security
• NIST 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
• NIST 800-64, Security Considerations in the Information System Development Life Cycle
• Framework for Improving Critical Infrastructure Cybersecurity