Agreement No. _____

AGREEMENT BETWEEN THE COUNTY OF SAN MATEO AND C3 AI

This Agreement is entered into this 19th day of April, 2022, by and between the County of San Mateo, a political subdivision of the state of California, hereinafter called "County" or "Sheriff's Office" or "Customer" and C3 AI, hereinafter called "Contractor." All capitalized terms used herein and not otherwise defined shall have the meaning set forth in Exhibit C.

* * *

Whereas, pursuant to Section 31000 of the California Government Code, County may contract with independent contractors for the furnishing of such services to or for County or any Department thereof; and

Whereas, it is necessary and desirable that Contractor be retained for the purpose of providing software and services to enable Intelligence Analysis Investigations Solution Software, a digital platform that will aggregate Sheriff's Office criminal investigation data sources and use artificial intelligence (AI) tools and analytics to help the Sheriff's Office build a unified, standardized view of criminal investigatory data, conduct criminal investigations, and assess its data faster.

Now, therefore, it is agreed by the parties to this Agreement as follows:

1. Exhibits and Attachments

The following exhibits and attachments are attached to this Agreement and incorporated into this Agreement by this reference:

Exhibit A—Order Form and Statement of Work (SOW)
Exhibit B—Payments and Rates
Exhibit C—C3 AI Additional Terms and Conditions
Exhibit D—California Department of Justice and County of San Mateo Data Security Policies
Exhibit E—Technical Specification C3001: C3 AI Suite, Applications, and Data Security

2. Services to be performed by Contractor

In consideration of the payments set forth in this Agreement and in Exhibit B, Contractor shall perform services for Sheriff's Office in accordance with the terms, conditions, and specifications set forth in this Agreement and in the Exhibits.

3. Payments

In consideration of the services provided by Contractor in accordance with all terms, conditions, and specifications set forth in this Agreement and in the Exhibits, County shall make payment to Contractor based on the rates and in the manner specified in Exhibit B. In no event shall County's total fiscal obligation under this Agreement exceed two million five hundred thousand dollars ($2,500,000.00).

4. Term

Subject to compliance with all terms and conditions, the term of this Agreement shall be from May 1, 2022, through April 30, 2027 (the "Term").

5. Termination

This Agreement may be terminated, as set forth below, by the Sheriff or the Sheriff's designee, for cause, including if Contractor's services do not meet the specifications and warranties in this Agreement and Exhibits. Subject to availability of funding, Contractor shall be entitled to receive payment for work/services provided prior to termination of the Agreement. Such payment shall be that prorated portion of the full payment determined by comparing the work/services actually completed to the work/services required by the Agreement. Notwithstanding the foregoing, County shall not be entitled to any refund of fees paid in the event of early termination of this Agreement by County.

County or Contractor may terminate this Agreement for cause. In order to terminate for cause, a party must first give the other party notice of the alleged breach. The party receiving notice shall have five (5) business days after receipt of such notice to respond and a total of ten (10) calendar days after receipt of such notice to cure the alleged breach. If the party receiving notice fails to cure the breach within this period, the party delivering notice may immediately terminate this Agreement without further action. In the event that a party provides notice of an alleged breach pursuant to this section, the party may, in extreme circumstances, immediately suspend performance of services and/or payment, as applicable, under this Agreement pending the resolution of the process described in this paragraph. Each party has sole discretion to determine what constitutes an extreme circumstance for purposes of this paragraph, and the party shall use reasonable judgment in making that determination.

6. Relationship of Parties

Contractor agrees and understands that the work/services performed under this Agreement are performed as an independent contractor and not as an employee of County and that neither Contractor nor its employees acquire any of the rights, privileges, powers, or advantages of County employees.

7. Hold Harmless

a. General Hold Harmless

Contractor shall indemnify and hold harmless the County and its officers, agents, employees, and servants from all claims, suits, or actions of every name, kind, and description resulting from this Agreement, the performance of any work or services required of Contractor under this Agreement, or payments made pursuant to this Agreement brought for, or on account of, any of the following:

(A) injuries to or death of any person, including Contractor or its employees/officers/agents;

(B) damage to any property of any kind whatsoever and to whomsoever belonging; or

(C) any other loss or cost, including but not limited to that caused by the concurrent active or passive negligence of County and/or its officers, agents, employees, or servants. However, Contractor's duty to indemnify and save harmless under this Section shall not apply to injuries or damage for which County has been found in a court of competent jurisdiction to be solely liable by reason of its own negligence or willful misconduct.

The duty of Contractor to indemnify and save harmless as set forth by this Section shall include the duty to defend as set forth in Section 2778 of the California Civil Code.

County will release and defend the Contractor against any claim, demand, suit or proceeding made or brought against the Contractor by a third party alleging that any of County Data infringes or misappropriates such third party's rights, or arising from County's use of Contractor's software in violation of this Agreement, including the Exhibits, or applicable law.

b. Intellectual Property Indemnification

Contractor hereby certifies that to its knowledge, it owns, controls, and/or licenses and retains all right, title, and/or interest in and to any intellectual property it uses in relation to this Agreement, including the design, look, feel, features, source code, content, and/or other technology relating to any part of the services it provides under this Agreement, including all related patents, inventions, trademarks, and copyrights, all applications therefor, and all trade names, service marks, know how, and trade secrets (collectively referred to as "IP Rights") except as otherwise noted by this Agreement.

Contractor warrants that the reports and similar results of the services, each as further described in the Statement of Work (SOW) that Contractor provides under this Agreement do not infringe, violate, trespass, or constitute the unauthorized use or misappropriation of any IP Rights of any third party. Contractor shall defend, indemnify, and hold harmless Sheriff's Office and San Mateo County from and against all liabilities, costs, damages, losses, and expenses (including reasonable attorney fees) in each case payable to a third party, arising out of or related to any claim by a third party that the services provided under this Agreement infringe or violate any third party's IP Rights provided any such right is enforceable in the United States.

Contractor's duty to defend, indemnify, and hold harmless under this Section applies only provided that: (a) County notifies Contractor within one week in writing of County's receipt of any notice of any such third-party claim; (b) County cooperates with Contractor, at Contractor's expense, in all reasonable respects in connection with the investigation and defense of any such third-party claim; (c) Contractor retains sole control of the defense of any action on any such claim and all negotiations for its settlement or compromise (provided Contractor shall not have the right to settle any criminal action, suit, or proceeding without County's prior written

consent, not to be unreasonably withheld, and provided further that any settlement permitted under this Section shall not impose any financial or other obligation on County, impair any right of County, or contain any stipulation, admission, or acknowledgement of wrongdoing on the part of County without County's prior written consent, not to be unreasonably withheld); and (d) should services under this Agreement become, or in Contractor's opinion be likely to become, the subject of such a claim, or in the event such a third party claim or threatened claim causes County's reasonable use of the services under this Agreement to be seriously endangered or disrupted, Contractor shall, at Contractor's option and expense, either: (i) procure for County the right to continue using the services without infringement or (ii) replace or modify the services so that they become non-infringing but remain functionally equivalent.

Notwithstanding anything in this Section to the contrary, Contractor will have no obligation or liability to County under this Section to the extent any otherwise covered claim is based upon: (a) any aspects of the services under this Agreement which have been modified solely by County without knowledge of Contractor in such a way as to cause the alleged infringement at issue; (b) any aspects of the services under this Agreement which have been used by County in a manner prohibited by this Agreement; (c) County's use of the C3 Materials in combination with any software, hardware, data, network or system not supplied by the Contractor, including County Data, where the alleged infringement or misappropriation relates to such combination and Contractor has advised Sheriff's Office against such a combination.

The duty of Contractor to indemnify and save harmless as set forth by this Section shall include the duty to defend as set forth in Section 2778 of the California Civil Code.

This Section 7 states the indemnifying Party's sole liability to, and the indemnified Party's exclusive remedy against, the other Party for any type of claim described in this Section 7.

c. Limitation of Liability

Excluding data breach and breaches of confidential information, the aggregate liability of each party, together with all of its affiliates and licensors, arising out of or related to this agreement shall not exceed four times the total amount of the agreement.

In no event will either party have any liability arising out of or related to this agreement for any lost profits, revenues, goodwill, or indirect, special, incidental, exemplary, consequential, cover, business interruption or punitive damages, whether an action is in contract or tort and regardless of the theory of liability, even if a party has been advised of the possibility of such damages or if a party's remedy otherwise fails of its essential purpose. The foregoing disclaimer will not apply to the extent prohibited by law.

8. Assignability and Subcontracting

Contractor shall not assign this Agreement or any portion of it to a third party or subcontract with a third party to provide services required by Contractor under this Agreement without the prior written consent of Sheriff's Office. Any such assignment or subcontract without prior written

consent of Sheriff's Office shall give County the right to automatically and immediately terminate this Agreement without penalty or advance notice.

9. Insurance

a. General Requirements

Contractor shall not commence work or be required to commence work under this Agreement unless and until all insurance required under this Section has been obtained and such insurance has been approved by County's Risk Management, and Contractor shall use diligence to obtain such insurance and to obtain such approval. Contractor shall furnish County with certificates of insurance evidencing the required coverage, and there shall be a specific contractual liability endorsement extending Contractor's coverage to include the contractual liability assumed by Contractor pursuant to this Agreement. These certificates shall specify or be endorsed to provide that thirty (30) days' notice must be given, in writing, to County of any pending change in the limits of liability or of any cancellation or modification of the policy.

b. Workers' Compensation and Employer's Liability Insurance

Contractor shall have in effect during the entire term of this Agreement workers' compensation and employer's liability insurance providing full statutory coverage. In signing this Agreement, Contractor certifies, as required by Section 1861 of the California Labor Code, that (a) it is aware of the provisions of Section 3700 of the California Labor Code, which require every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of the Labor Code, and (b) it will comply with such provisions before commencing the performance of work under this Agreement.

c. Liability Insurance

Contractor shall take out and maintain during the term of this Agreement such bodily injury liability and property damage liability insurance as shall protect Contractor and all of its employees/officers/agents while performing work covered by this Agreement from any and all claims for damages for bodily injury, including accidental death, as well as any and all claims for property damage which may arise from Contractor's operations under this Agreement, whether such operations be by Contractor, any subcontractor, anyone directly or indirectly employed by either of them, or an agent of either of them. Such insurance shall be combined single limit bodily injury and property damage for each occurrence and shall not be less than the amounts specified below:

(a) Comprehensive General Liability	$1,000,000
(b) Motor Vehicle Liability Insurance	$1,000,000
(c) Professional Liability .	$1,000,000
(d) Cyber Liability Insurance	$5,000,000

County and its officers, agents, employees, and servants shall be named as additional insured on any such policies of insurance, which shall also contain a provision that (a) the insurance afforded thereby to County and its officers, agents, employees, and servants shall be primary insurance to the full limits of liability of the policy and (b) if the County or its officers, agents, employees, and servants have other insurance against the loss covered by such a policy, such other insurance shall be excess insurance only.

In the event of the breach of any provision of this Section, or in the event any notice is received which indicates any required insurance coverage will be diminished or canceled, County, at its option, may, notwithstanding any other provision of this Agreement to the contrary, immediately declare a material breach of this Agreement and suspend all further work and payment pursuant to this Agreement.

d. Cyber Liability Insurance

Privacy and Network Security: During the term of the Contract and for three years thereafter, Countractor will maintain coverage for liability and remediation arising out of unauthorized use of or access to County Data or software within Contractor's network or control. Contractor's insurance will provide coverage for liability claims, computer theft, extortion, network breach, service denial, introduction of malicious code, loss of confidential information, or any unintentional act, error, or omission made by users of Contractor's electronic data or systems while providing services to the County. The insurance policy must include coverage for regulatory and PCI fines and penalties, crisis management expenses, and business interruption. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

10. Compliance With Laws

All services to be performed by Contractor pursuant to this Agreement shall be performed in accordance with all applicable Federal, State, County, and municipal laws, ordinances, and regulations, including but not limited to the Americans with Disabilities Act of 1990, as amended, and Section 504 of the Rehabilitation Act of 1973, which prohibits discrimination on the basis of disability in programs and activities receiving any Federal or County financial assistance. Such services shall also be performed in accordance with all applicable ordinances and regulations, including but not limited to appropriate licensure, certification regulations, provisions pertaining to confidentiality of records, and applicable quality assurance regulations. In the event of a conflict between the terms of this Agreement and any applicable State, Federal, County, or municipal law or regulation, the requirements of the applicable law or regulation will take precedence over the requirements set forth in this Agreement.

Further, Contractor certifies that it and all of its subcontractors will adhere to all applicable provisions of Chapter 4.106 of the San Mateo County Ordinance Code, which regulates the use of disposable food service ware. Accordingly, Contractor shall not use any non-recyclable plastic disposable food service ware when providing prepared food on property owned or leased by the County and instead shall use biodegradable, compostable, reusable, or recyclable plastic food service ware on property owned or leased by the County.

Contractor will timely and accurately complete, sign, and submit all necessary documentation of compliance.

11. Non-Discrimination and Other Requirements

a. General Non-discrimination

No person shall be denied any services provided pursuant to this Agreement (except as limited by the scope of services) on the grounds of race, color, national origin, ancestry, age, disability (physical or mental), sex, sexual orientation, gender identity, marital or domestic partner status, religion, political beliefs or affiliation, familial or parental status (including pregnancy), medical condition (cancer-related), military service, or genetic information.

b. Equal Employment Opportunity

Contractor shall ensure equal employment opportunity based on objective standards of recruitment, classification, selection, promotion, compensation, performance evaluation, and management relations for all employees under this Agreement. Contractor's equal employment policies shall be made available to County upon request.

c. Section 504 of the Rehabilitation Act of 1973

Contractor shall comply with Section 504 of the Rehabilitation Act of 1973, as amended, which provides that no otherwise qualified individual with a disability shall, solely by reason of a disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination in the performance of any services this Agreement. This Section applies only to contractors who are providing services to members of the public under this Agreement.

d. Compliance with County's Equal Benefits Ordinance

Contractor shall comply with all laws relating to the provision of benefits to its employees and their spouses or domestic partners, including, but not limited to, such laws prohibiting discrimination in the provision of such benefits on the basis that the spouse or domestic partner of the Contractor's employee is of the same or opposite sex as the employee.

e. Discrimination Against Individuals with Disabilities

The nondiscrimination requirements of 41 C.F.R. 60-741.5(a) are incorporated into this Agreement as if fully set forth here, and Contractor and any subcontractor shall abide by the requirements of 41 C.F.R. 60–741.5(a). This regulation prohibits discrimination against qualified individuals on the basis of disability and requires affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified individuals with disabilities.

f. History of Discrimination

Contractor certifies that no finding of discrimination has been issued in the past 365 days against Contractor by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other investigative entity. If any finding(s)

of discrimination have been issued against Contractor within the past 365 days by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or other investigative entity, Contractor shall provide County with a written explanation of the outcome(s) or remedy for the discrimination prior to execution of this Agreement. Failure to comply with this Section shall constitute a material breach of this Agreement and subjects the Agreement to immediate termination at the sole option of the County.

g. Reporting; Violation of Non-discrimination Provisions

Contractor shall report to the County Manager the filing in any court or with any administrative agency of any complaint or allegation of discrimination on any of the bases prohibited by this Section of the Agreement or the Section titled "Compliance with Laws". Such duty shall include reporting of the filing of any and all charges with the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other entity charged with the investigation or adjudication of allegations covered by this subsection within 30 days of such filing, provided that within such 30 days such entity has not notified Contractor that such charges are dismissed or otherwise unfounded. Such notification shall include a general description of the circumstances involved and a general description of the kind of discrimination alleged (for example, gender-, sexual orientation-, religion-, or race-based discrimination).

Violation of the non-discrimination provisions of this Agreement shall be considered a breach of this Agreement and subject the Contractor to penalties, to be determined by the County Manager, including but not limited to the following:

i. termination of this Agreement;
ii. disqualification of the Contractor from being considered for or being awarded a County contract for a period of up to 3 years;
iii. liquidated damages of $2,500 per violation; and/or
iv. imposition of other appropriate contractual and civil remedies and sanctions, as determined by the County Manager.

To effectuate the provisions of this Section, the County Manager shall have the authority to offset all or any portion of the amount described in this Section against amounts due to Contractor under this Agreement or any other agreement between Contractor and County.

h. Compliance with Living Wage Ordinance

As required by Chapter 2.88 of the San Mateo County Ordinance Code, Contractor certifies all contractor(s) and subcontractor(s) obligated under this contract shall fully comply with the provisions of the County of San Mateo Living Wage Ordinance, including, but not limited to, paying all Covered Employees the current Living Wage and providing notice to all Covered Employees and Subcontractors as required under the Ordinance.

12. Compliance with County Employee Jury Service Ordinance

Contractor shall comply with Chapter 2.85 of the County's Ordinance Code, which states that Contractor shall have and adhere to a written policy providing that its employees, to the extent they are full-time employees and live in San Mateo County, shall receive from the Contractor, on an annual basis, no fewer than five days of regular pay for jury service in San Mateo County, with jury pay being provided only for each day of actual jury service. The policy may provide that such employees deposit any fees received for such jury service with Contractor or that the Contractor may deduct from an employee's regular pay the fees received for jury service in San Mateo County. By signing this Agreement, Contractor certifies that it has and adheres to a policy consistent with Chapter 2.85. For purposes of this Section, if Contractor has no employees in San Mateo County, it is sufficient for Contractor to provide the following written statement to County: "For purposes of San Mateo County's jury service ordinance, Contractor certifies that it has no full-time employees who live in San Mateo County. To the extent that it hires any such employees during the term of its Agreement with San Mateo County, Contractor shall adopt a policy that complies with Chapter 2.85 of the County's Ordinance Code." The requirements of Chapter 2.85 do not apply if this Agreement's total value listed in the Section titled "Payments", is less than one-hundred thousand dollars ($100,000), but Contractor acknowledges that Chapter 2.85's requirements will apply if this Agreement is amended such that its total value meets or exceeds that threshold amount.

13. Retention of Records; Right to Monitor and Audit

(a) Contractor shall maintain all required records relating to services provided under this Agreement for three (3) years after County makes final payment and all other pending matters are closed, and Contractor shall be subject to the examination and/or audit by County, a Federal grantor agency, and the State of California.

(b) Contractor shall comply with all program and fiscal reporting requirements set forth by applicable Federal, State, and local agencies and as required by County.

(c) Contractor agrees upon reasonable notice to provide to County, to any Federal or State department having monitoring or review authority, to County's authorized representative, and/or to any of their respective audit agencies reasonable access to and the right to examine relevant records and documents necessary to determine compliance with relevant Federal, State, and local statutes, rules, and regulations, to determine compliance with this Agreement, and to evaluate the quality, appropriateness, and timeliness of services performed.

14. Merger Clause; Amendments

This Agreement, including the Exhibits and Attachments attached to this Agreement and incorporated by reference, constitutes the sole Agreement of the parties to this Agreement and correctly states the rights, duties, and obligations of each party as of this document's date. In the event that any term, condition, provision, requirement, or specification set forth in the body of this Agreement conflicts with or is inconsistent with any term, condition, provision, requirement, or specification in any Exhibit and/or Attachment to this Agreement, the provisions

of the body of the Agreement shall prevail. Any prior agreement, promises, negotiations, or representations between the parties not expressly stated in this document are not binding. All subsequent modifications or amendments shall be in writing and signed by the parties. Terms used in the Agreement or any Exhibits may be used in the others.

15. Controlling Law; Venue

The validity of this Agreement and of its terms, the rights and duties of the parties under this Agreement, the interpretation of this Agreement, the performance of this Agreement, and any other dispute of any nature arising out of this Agreement shall be governed by the laws of the State of California without regard to its choice of law or conflict of law rules. Any dispute arising out of this Agreement shall be venued either in the San Mateo County Superior Court or in the United States District Court for the Northern District of California.

Without limiting the foregoing, County and the Contractor agree that damages will be an inadequate remedy in the case of any actual or threatened breach of certain terms of this Agreement or any exhibits (including any unauthorized disclosure of Confidential Information), and that County or the Contractor may therefore seek equitable relief in addition to any other remedies it may have for such breach with any competent court or enforcement agencies, including those in the United States and/or in the country in which County is domiciled, without bond and without necessity of showing monetary damages. County and the Contractor agree that the United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Transactions Act are specifically excluded from application to this Agreement.

16. Notices

Any notice, request, demand, or other communication required or permitted under this Agreement shall be deemed to be properly given when both: (1) transmitted via facsimile to the telephone number listed below or transmitted via email to the email address listed below; and (2) sent to the physical address listed below by either being deposited in the United States mail, postage prepaid, or deposited for overnight delivery, charges prepaid, with an established overnight courier that provides a tracking number showing confirmation of receipt.

In the case of County, to:

Name/Title:	Kimberly Honciano, Director of Technology Services
Address:	400 County Center, 3rd Floor, Redwood City, CA 94063
Telephone:	(650) 599-1711
Facsimile:	(650) 599-1327
Email:	khonciano@smcgov.org

and

Name/Title:	Mark Duri, Assistant Sheriff
Address:	400 County Center, 3rd Floor, Redwood City, CA 94063

Telephone: (650) 363-4498
Facsimile: (650) 599-1327
Email: mduri@smcgov.org

In the case of Contractor, to:

Name/Title: General Counsel
Address: 1300 Seaport Blvd, Suite 500, Redwood City, CA 94063
Telephone: (650) 503-2200

Email: C3legal@c3.ai

17. Electronic Signature

Both County and Contractor wish to permit this Agreement and future documents relating to this Agreement to be digitally signed in accordance with California law and County's Electronic Signature Administrative Memo. Any party to this Agreement may revoke such agreement to permit electronic signatures at any time in relation to all future documents by providing notice pursuant to this Agreement.

18. Payment of Permits/Licenses

Contractor bears responsibility to obtain any license, permit, or approval required from any agency for work/services to be performed under this Agreement at Contractor's own expense prior to commencement of said work/services. Failure to do so will result in forfeit of any right to compensation under this Agreement.

* * *

In witness of and in agreement with this Agreement's terms, the parties, by their duly authorized representatives, affix their respective signatures:

For Contractor: C3 AI

Richard J. Lutton Jr.	March 24, 2022	C3.ai, Inc. by Richard J. Lutton, Jr. SVP & General Counsel
Contractor Signature	Date	Contractor Name (please print)

COUNTY OF SAN MATEO

By:

President, Board of Supervisors, San Mateo County

Date:

ATTEST:

By:

Clerk of Said Board

Exhibit A

Order Form

THIS ORDER FORM (this "**Order Form**") sets out the order of certain software subscription and services made by the County.

I. **Commercial Terms**

a. Order Form Effective Date: the date listed in the Agreement as the beginning of the Term

b. Subscription Term: Five (5) years commencing on the Order Form Effective Date

c. Deployment Environment: County AWS Account

d. Fees: As specified in Exhibit B

II. **Order.** *In consideration of the payments set forth in Exhibit B, Contractor shall provide the following:*

a. **C3 AI Intelligence Analysis Application** subscription for the Subscription Term, deployed in the Deployment Environment

b. **C3 Implementation Services,** as specified in the below Statement of Work, attached as Annex A-1.

c. **C3 Support Services**, as defined in Exhibit C throughout the Subscription Term

III. **Other Professional Services.** All additional services requested by County, including without limitation any professional or consulting services shall be subject to a separate mutually agreed Statement of Work and at C3 AI's standard professional services rates.

Annex A-1: Statement of Work

1. Introduction

THIS STATEMENT OF WORK (this "**SOW**") describes the Implementation Services C3 AI may perform to configure and deploy a production C3 AI Intelligence Analysis Application ordered under the Agreement. This SOW is subject to and made a part of the Agreement. To the extent the terms of the Agreement with respect to the scope of the Project (as defined below) conflict with the terms and conditions of this SOW, this SOW shall control. Capitalized terms used but not defined in this SOW shall have the meaning ascribed to them in the Agreement or in the Order Form.

2. Project Scope

This project scope is limited to configuring and deploying into production the C3 AI IA application with four previously identified data sources and up to 4 UI screens ("Wave 1"), and then to add an additional eight (8) additional data sources (the "In-Scope Data") ("Wave 2").

The previously configured four data sources for the pilot will go live within three months of the date of contract execution and the remaining eight data sources will go live within twelve months of the date of contract execution.

3. Data Integration

Data integration is a critical requirement for successful project completion. C3's obligation to perform its data integration is contingent upon Customer's successful transfer of accurately formatted data from its source systems to C3. The data will include the data elements defined in Table 1, below. Changing the data sources listed in Table 1 to substitute alternate sources with similar levels of integration complexity (e.g. APIs) will not, by itself, activate the formal change control process described in Section 7, below.

Table 1. In-Scope Data

Data Sources	Description	Integration Points (e.g., ReST API, RDBMS)	In Pilot or New Integration (Deployment Phase)
ATIMS	Records of jail inmates and associated activities	RDBMS	In Pilot (Phase 0)

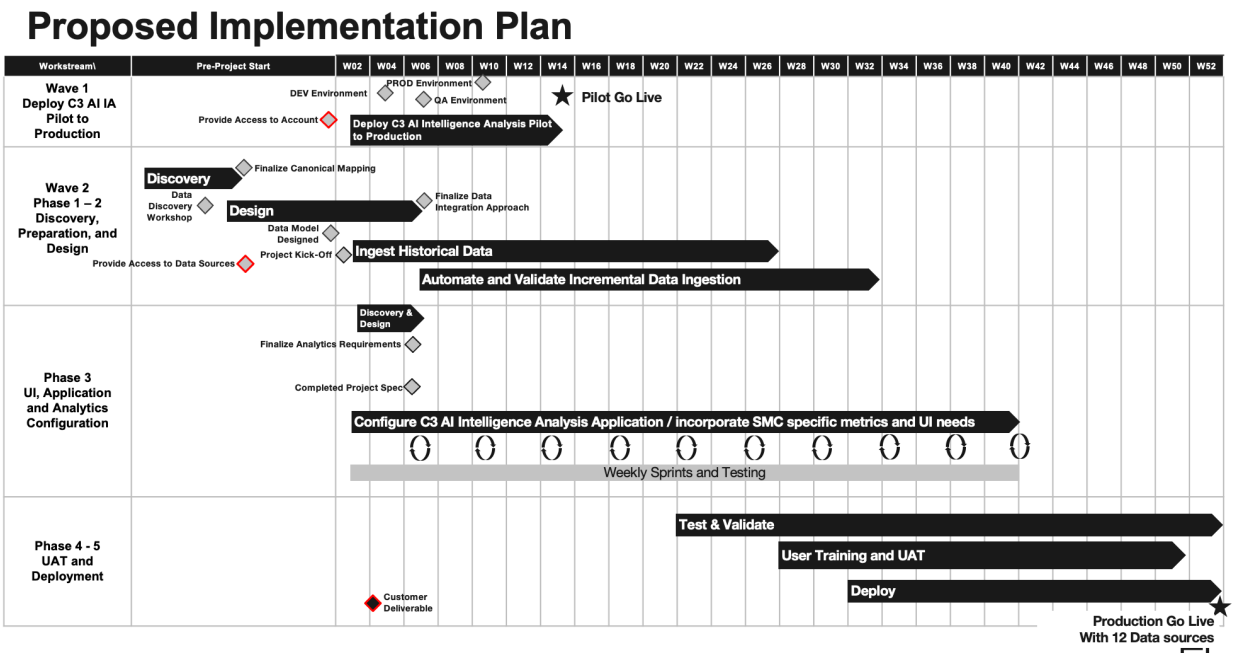
	(e.g., admission date, release date, visitations)		
Sunridge RIMS	Records associated with criminal investigations – including citations, warrants, crime reports, and case numbers	RDBMS	In Pilot (Phase 0)
Axon Technologies Evidence.com	Video footage associated with crime reports and associated case numbers (e.g., body cameras, in-vehicle cameras, interviews)	API to SMC SO's account on Evidence.com	In Pilot (Phase 0)
Vigilant ALPR	License plate images and recognition data (e.g., license plate number, violation date and location)	API to SMC SO's account on Vigilant	In Pilot (Phase 0)
Versaterm vCAD	Records from computer aided dispatch system	TBD	New Integration (Phase 1)
Digital Reel	Digitized microfilm records	FTP or API to SMC SO's account on Digital Reel	New Integration (Phase 1)
Odyssey	Criminal justice integration system for court records	API or through SMC SO Middleware layer	New Integration (Phase 1)
Prosecutor by Karpel (PBK)	Records for district attorney case management system	PBK Law Enforcement Interface	New Integration (Phase 1)
CalPhoto	California DMV driver's license photos	TBD	New Integration (Phase 1)
TransUnion TLOxp	Identity data for criminals, suspects, and fugitives	API	New Integration (Phase 1)

IC Solutions	Call records for jail inmates	TBD	New Integration (Phase 1)
APBNet-TRAK	National law enforcement alert and information sharing bulletins	TBD	New Integration (Phase 1)

4. Project Timeline

C3 and Customer will use the data model, data format, and transport pipeline being built for the C3 AI IA pilot application. The Customer will provide in-scope historical and incremental data in an ingestible format and with quality required by C3. Any mis-formatting of data, data quality issues, or delays in delivering data, including without limitation any delay by Customer to deliver the complete set of data to C3 in an ingestible format will result in delays and may incur additional fees at the prevailing professional services rates.

Figure 1. Project Timeline



The Project will have the following phases for Wave 2.

Phase 1: Discovery

- C3 Responsibilities:
    a. Joint data discovery and review
    b. Provide detailed project plan
    c. Conduct data discovery workshop
    d. Provide data integration requirements
- Customer Responsibilities:

a. Provide SMEs to participate in data discovery and review
b. Finalize data sources and fields

Phase 2: Design

- C3 Responsibilities:
  a. Finalize data integration requirements
  b. Develop Specifications for UI Configuration, and metrics
- Customer Responsibilities:
  a. Design data mapping and transforms from source systems to C3 AI IA

Phase 3: Configuration

- C3 Responsibilities:
  a. Ingest historical and incremental Data for In-Scope Data
  b. Test UI and C3 Application configuration
- Customer Responsibilities:
  a. Provide in-scope historical and incremental data in a pre-defined canonical format and with required quality

Phase 4: Test and Validate

- C3 Responsibilities:
  a. Deliver UAT test plan
  b. Deliver Customer-specific end-user training to UAT testers
  c. Execute Integration Testing
  d. Execute PSR Testing
  e. Complete production readiness activities (e.g., deployment plan, production data cutover)
- Customer Responsibilities:
  a. Provide SMEs to support end-to-end testing
  b. Conduct UAT Testing
  c. Provide UAT Sign-Off

Phase 5: Deploy

- C3 Responsibilities:
  a. Conduct (1) “Train-the-Trainer” end-user training with Customer-specific training materials
  b. Deploy to Production
- Customer Responsibilities:
  a. Identify “Train-the-Trainer” participants

During the Project, C3 will hold a series of workshops and meetings. The workshops are collaborative sessions between C3 and Customer project teams for refining requirements, schedule, deliverables and resolving key challenges. Table 2 below summarizes the planned workshops and reoccurring meetings and their objectives.

Table 2. Planned Workshops and Meetings

Key Workshops	Objectives
Project Kick-off	Validate scope, review Project plan, implementation approach and milestones
Data Discovery	Review data requirements and C3 Canonical Data Model to enable Customer to conduct historical data extraction and perform transformation to adhere to C3 Canonical Data Model
Data Integration Design	Finalize data integration architecture; enable Customer to develop automated integration infrastructure
Design Review	Approve the overall configuration design
Model Validation Checkpoint	Review preliminary machine learning model output and gather Customer feedback to further refine
Post-Deployment Debriefing	Review and close any new issues after the Production Release
Meeting	**Objectives**
Quarterly Executive Reviews	Customer and C3 Executive Sponsors meet to review Project progress, address issues, and assign necessary resources
Weekly Status Meetings	Customer and C3 Project teams meet to review Project status, discuss technical questions, track risks/mitigation steps, and resolve issues

5. Deliverables

Table 3 below summarize the Project Deliverables which will be completed across Wave 1 and Wave 2.

Table 3: Project Deliverables

ID	Deliverable	Implementation Phase	Responsible Party
1	Project Plan • Detailed Project plan	Discovery	C3
2	C3 Canonical Workbook • Documentation of extensions to C3 canonicals and mapping between C3 canonical entities and Customer source systems • This will be completed as an output of the Data Discovery Workshop	Discovery	C3
3	Functional Specifications • Specifications for UI configuration and application analytics	Design	C3
4	Application Design Specifications • Documentation of data integration architecture and agreed-to schema	Design	C3
5	QA Release • Release of QA environment for Customer UAT	Configuration	C3
6	UAT Test Plan • Description of the UAT test plan, test scenarios, timeline and exit criteria	Validation	C3
7	Go-Live Deployment Plan • Deliverable includes the schedule, tasks, and key responsibilities for the activities leading up to the production deployment of the C3 Application	Validation	C3
8	Production Release • Deliver production ready C3 Application	Deployment	Customer
9	Training • C3 will conduct (1) “train-the-trainer” training and provide the Customer-specific user training manual for each of the configured C3 AI Intelligence Analysis Application	Train	C3

6. Project Personnel

The project team will be comprised of trained C3 and Customer personnel to fulfill the project resource requirements. Table 4 below details the minimum personnel roles and responsibilities required to be assigned to the project.

Table 4: Project Resource Requirements

Role Title	Source
Project Executive Sponsors: Holds ultimate responsibility for delivering the project on time and on budget	C3
	Customer
Project Manager: Manages the day-to-day activities of Project team.	C3
	Customer
Data Integration Specialists: Performs data integration and testing, advises Customer on data model and mapping to source systems, extends C3 canonical model	C3
Product Manager: Designs and develops the C3 AI Suite, Tools, and C3 Applications roadmap	C3
Application Development Engineers: Designs, develops, and configures C3 solutions	C3
Data Scientists: Develops and validates application analytics	C3
IT Architects/Developers: Designs the conversion and batch extractions to provide data and access to all source data and systems to C3	Customer
Subject Matter Experts: subject matter experts as required including business and IT technical leads	Customer

7. Constraints

Below is a list of constraints that includes the obligations for which Customer is responsible and assumptions upon which C3 have agreed to perform the C3 Implementation Services on the terms set out herein (collectively "**Customer Obligations**"). If any of Customer Obligations are not performed or prove to be incorrect, this may cause changes to the schedule, fees, deliverables, and level of effort required, in addition to impacting C3 performance of the services described herein.

A. Customer will deliver complete In-Scope Data (minimum 2 years of historical data and incremental data) sent to C3 in the agreed-upon format and with the required data quality at the start of the Project for Wave 2.

B. All timelines included in this SOW assume that the Project begins on the later date that (a) C3 receives all In-Scope Data in the agreed format with the required data quality (i.e., data with no transformations), and (b) C3 receives the calculation logic for any data or functions that need to be derived from the source (a and b, collectively, "Data Delivery").

C. Any data formatting errors or inconsistencies, data quality issues, or delays in Data Delivery may delay the Deployment and incur incremental fees. Any incremental fees will be approved by Customer before they are incurred and/or invoiced.

D. Customer shall be responsible for its contractual relationships with third parties and shall be responsible for such third parties' cooperation to carry out the obligations herein.

E. Customer will be responsible for providing the Customer resources necessary to fulfill the Customer-identified work and responsibilities outlined in Section 4 above

F. Customer will provide licenses identified as necessary from third parties required for C3 to perform its obligations in this SOW. C3 agree to comply with license terms and conditions.

G. The C3 Application is required to be utilized with a Google Chrome web browser.

H. Customer is responsible for supporting definition, review and approval of functional specifications, including metrics.

I. Customer will comply with the Operational Controls set forth in Appendix B.

8. Change Control Process

Should either Party wish to alter the content of this Statement of Work, the following procedure will apply. This process will not be activated, however, solely as a result of changes to the in-scope data sources listed in Table 1 of section 3, above. The person who requests the change (the "**Requestor**") will forward to the other party (the "**Recipient**") a Change Order, which will include the following:

1. Party's Name
2. Requestor's name and title
3. Date Requested
4. Priority level of the request as either Priority 1 (Urgent) or Priority 2 (Ordinary)
5. A description of the proposed change
6. The reason for the proposed change

C3 will complete an impact analysis with the Customer to determine the impact to the Project schedule or budget for review and subsequent signatures if approved. Both parties must agree in writing before this Change Order can be executed and resources scheduled to complete

work. A Change Order should be completed, even if the impact is negligible, to document any and all change in scope.

Escalation Process

The following section addresses the escalation process for some common situations that may arise during the course of this Project.

Change Order – Should a Change Order become delayed, the processes listed below will be followed to remediate the situation:

Situation	Responsible Personnel	Process
Change Order process has been delayed 1 to 5 business days	1. C3 Project Manager 2. Customer Project Sponsor	Work jointly to determine remediation steps and complete change order process
Change Order process has been delayed in excess of 5 business days	1. C3 Executive Sponsor 2. Customer Executive Sponsor	Work jointly with Project Managers to determine remediation steps and complete change order process

Project Delays – In case of any Project delays, the Parties will follow the following escalation process:

Situation	Responsible Personnel	Process
Anticipated delays	1. C3 Project Manager 2. Customer Project Sponsor	Standard Change Order process
Actual delays of 1 to 5 business days	1. C3 Project Manager 2. Customer Project Sponsor	Work jointly to determine impact with possible remediation steps, and complete Change Order process
Actual delays in excess of 5 business days	1. C3 Executive Sponsor 2. Customer Executive Sponsor	Work jointly with Project Managers to determine impact with possible remediation steps, and complete Change Order process

Quality of Work or Technical Implementation Issues – All services performed by C3 are warranted as provided in the Agreement. If the Customer or C3 should have any concerns about the quality of work or technical implementation, the processes listed below will be followed to remediate the situation:

Situation	Responsible Personnel	Process
Quality of Work	1. C3 Project Manager 2. Customer Project Sponsor	Work jointly to determine remediation of any issues related to quality of work
Technical Implementation	1. C3 Technical Personnel 2. Customer Technical Lead	Work jointly with Project Managers to determine best practices for technical implementation and remediate discrepancies
Technical Solution	1. C3 Account Director 2. Customer Project Sponsor	Work jointly with Project Managers and Technical Subject Matter Experts to determine the best path forward to resolve conflict

Any dispute that is unresolved after 5 business days	1. C3 Executive Sponsor 2. Customer Executive Sponsor	Work jointly with Project Managers to determine remediation of any issues related to quality of work, technical implementation, or technical solution

Exhibit B

Payments and Rates

In consideration of the services provided by Contractor described in Exhibit A and subject to the terms of the Agreement, County shall pay Contractor based on the following fee schedule and terms:

The total cost of the products and services ordered in Exhibit A shall not exceed $2,500,000 for 5 years. Each payment shall be invoiced by Contractor upon the applicable Payment Date set forth below, and shall be payable in full within 30 days of the invoice. County is responsible for providing complete and accurate billing and contact information and notifying Contractor of any changes to this information.

Table 1

C3 AI Line Items	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
C3 AI Intelligence Analysis Application Subscription Fees	Included				
C3 Pre-paid Runtime* *(up to 1.5 million vCPU hours included annually)*	Included*				
C3 Implementation Services**	Included**				
C3 Support Services	Included				
Total Fees per Year	**$500,000**	**$500,000**	**$500,000**	**$500,000**	**$500,000**
TOTAL Fees (5-year Term)	**$2,500,000**				

*Once the Pre-Paid Runtime is exhausted, County will be invoiced as incurred, monthly in arrears, for C3 Runtime at the standard C3 Runtime rates**.** Excludes County's Hosting Services Fees.

**C3 Implementation Services as described in Exhibit A, only.

The total fees for products and services ordered in Exhibit A during the Subscription Term are $2,500,000. The Total Fees will be invoiced as follows: (i) $500,000 on the Effective Date; (ii) $500,000 on the first anniversary of the Effective Date; (iii) $500,000 on the second anniversary of the Effective Date; (iv) $500,000 on the third anniversary of the Effective Date; and (v) $500,000 on the fourth anniversary of the Effective Date.

"**C3 Runtime**" means vCPU and vGPU usage in production environments by C3 AI Application(s) and does not include Hosting Services fees. The Pre-Paid C3 Runtime Fees set forth in Table 1 ("**Pre-Paid C3 Runtime Fees**") reflect County's purchase of C3 Runtime in advance up to a defined annual maximum. Beyond the prepaid maximum, fees for C3 Runtime are calculated by multiplying County's C3 Runtime during the month by the applicable C3 Runtime rates.

C3 Runtime used by the County is credited against the Pre-Paid Runtime until the Pre-Paid Runtime is exhausted. Any Pre-Paid C3 Runtime not used during the applicable period expire at the end of that period, and does not "rollover" or apply as a credit against any fees for C3 Runtime due in the following or preceding periods. Once the Pre-Paid Runtime is exhausted, County will incur and be invoiced monthly in arrears for C3 Runtime Fee at the standard C3 Runtime rates set forth below:

Standard C3 Runtime rates	**$0.22/vCPU per hour**
	$1.40/vGPU per hour

County may purchase additional blocks of pre-paid C3 Runtime by entering into a separate transaction with C3 AI. C3 will provide monthly Runtime usage reports throughout the Term.

C3 Support Services. C3 Support Services (described in Exhibit C, below) for the C3 AI Intelligence Analysis Application are included during the Subscription Term upon County's payment of the fees due under this Order Form.

If any amount owing by County under this Agreement is 30 or more days overdue, C3 AI may, without limiting C3 AI's other rights and remedies, suspend any services it is providing to County until such amounts are paid in full. C3 AI will give County at least 10 days prior written notice that County's account is overdue, before suspending services to County. C3 AI will not exercise the rights under this section if County is disputing the applicable charges reasonably and in good faith and are cooperating diligently to resolve the dispute.

Exhibit C

ADDITIONAL TERMS AND CONDITIONS

C3 AI Subscription and Services Terms & Conditions (including Annexes C-1, C-2, and C-3)

This **C3 AI Subscription and Services Terms and Conditions** shall be incorporated by reference and will form a part of the Agreement entered into by and between the Contractor and the County on the date hereof.

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly is controlled by, or is under common control with, the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Beta Services**" means Contractor's services or functionality designated as a beta, pilot, limited release, developer preview, non-production, evaluation or by similar description, that Contractor may make available to County at County's option.

"**C3 Application**" means Contractor's hosted software application(s), if any, specified on an Order Form.

"**C3 Implementation Services**" means implementation services, if any, described in a mutually agreed order form or statement of work ("**Statement of Work**").

"**C3 Materials**" means (i) Contractor's Applications, Documentation, Confidential Information, and the results of C3 Implementation Services or C3 Support Services; (ii) C3 Pre-Existing Materials and any modifications and derivative works thereof; and (iii) any and all other Intellectual Property, including Intellectual Property Rights therein, developed by or on behalf of Contractor.

"**C3 Pre-existing Materials**" means Contractor's Intellectual Property, that exists as of the Effective Date or is developed after the Effective Date independently of the Agreement.

"**C3 Services**" means individually and collectively, the C3 Applications, C3 Implementation Services and C3 Support Services that County orders from C3 AI pursuant to an Order Form or Statement of Work, but excludes Third Party Offerings.

"**C3 Support Services**" means the support services described in Annex C-1, if ordered pursuant to an applicable Order Form.

"**County Data**" means all electronic data and electronic information submitted by or for County to be processed on or by the C3 Applications.

"**Data Security Technical Specification"** means Contractor's cyber security program document entitled "Technical Specification C3001: C3 Platform, Applications, and Data Security," as may be updated from time to time by Contractor.

"**Documentation**" means any user documentation made available by Contractor for the applicable C3 Application.

"**Hosting Services**" means the infrastructure and related services, including online data storage and computation services, provided by a third party hosting service provider selected or approved by Contractor from time to time.

"**Intellectual Property**" means any and all intellectual and industrial property and tangible embodiments thereof, including, without limitation, inventions, discoveries, computer programs in machine readable object code form and source code form, compilations of data and computer databases, algorithms, scripts, templates, specifications, designs, methods, know-how, processes, trade secrets, confidential information, works of authorship, mask works and integrated circuit topographies, modifications and improvements.

"**Intellectual Property Rights**" means, collectively, all rights in, to and under patents, trade secret rights, copyrights, trademarks, service marks, moral rights and other similar rights of any type under the laws of any governmental authority, including without limitation rights in the applications and registrations relating to the foregoing.

"**Malicious Code**" means code, files, scripts, agents or programs intended to do harm, including, for example, viruses, worms, time bombs and Trojan horses.

"**Order Form**" means one or more ordering document(s) that specify the Subscribed or purchased Contractor Service(s) that are entered into between Contractor and County, including any Statement of Work and other addenda incorporated therein.

"**Provision**" or "**Provisioning**" means the process for on-boarding or establishing access to users of cloud-based software applications.

"**Subscribe**" or "**Subscribed**" means County has timely paid all applicable fees agreed in an Order Form and is otherwise in compliance with its obligations under the Agreement and the Order Form.

"**Third Party Offering**" means any software or services that County licenses or procures from a third party that County uses in connection with, or which interoperates with, any C3 Application.

"**User**" means an individual employee or subcontractor of County Sheriff's office who is authorized by County to access or use a Subscribed C3 Service, and to whom County (or, when applicable, Contractor at County's request) has supplied a user identification and password.

2. C3 AI's RESPONSIBILITIES

2.1. **Provisioning of C3 Applications**. Subject to the terms of this Agreement, Contractor will (a) Provision in the Hosting Services environment, during the applicable Subscription Term (as defined in Section 3.1 below), the C3 Application(s) to which County has Subscribed, and (b) in connection therewith, provide C3 Support Services to County.

2.2. **Contractor's Personnel**. Contractor will be responsible for the performance of its personnel (including Contractor's employees and sub-contractors) and their compliance with Contractor's obligations under the Agreement, except as otherwise specified herein. Contractor's personnel will be obligated to comply with all requirements of the Criminal Justice Information Services (CJIS) Security Policy, as set forth in Exhibit D.

3.

3.1. **Beta Services.** From time to time, Contractor may make Beta Services available to County at no charge. County may choose to try such Beta Services, in County's sole discretion. Beta Services (i) are intended for and may only be used by County for evaluation purposes only and not for production use, (ii) are not supported by Contractor, and (iii) may be subject to additional terms. In addition to the foregoing limitations, all use of the Beta Services is subject to all other terms and conditions that apply to C3 Services, including without limitation Contractor's reservation of all rights and County's obligations and restrictions on use concerning the C3 Services, and use of any related Third Party Offerings. Unless otherwise stated, any Beta Services trial period will expire upon the earlier of, one year from the trial start date, the date that a version of the Beta Services becomes generally available without the applicable Beta Services designation, or when terminated by Contractor. Contractor may discontinue Beta Services at any time in Contractor's sole discretion and may never make them generally available. Beta Services are provided "as is" and may contain bugs or errors. Contractor will have no liability for any warranties, harm or damage arising out of or in connection with a Beta Service.

3.2. **Future Functionality**. County agrees that County's purchases are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by C3 AI regarding future functionality or features.

4. USE OF C3 SERVICES

4.1. **Services**. Unless otherwise provided in the applicable Order Form or Documentation, C3 Services (other than C3 Implementation Services) are purchased as subscriptions for the term specified in an Order Form ("**Subscription Term**"). Subject to County's compliance with this Agreement and the applicable Order From, County has the right, during the applicable Subscription Term, to access and use the C3 Materials for County's internal business purposes only within the scope specified in the applicable Order Form. County may permit the number of Users specified in the applicable Order Form (or, if no number is specified in the Order Form, an unlimited number of Users) to use, but not develop or modify, the C3 Applications internally at the County for County's internal business purposes.

4.2. **Service Level Agreement**. Contractor will use commercially reasonable efforts to make the Subscribed C3 Materials available as set forth in Annex C-2.

4.3. **County's Responsibilities**. County will (i) be responsible for Users' compliance with this Agreement, Documentation, and Order Forms, (ii) be responsible for the accuracy, quality, and legality of County Data and the means by which County acquired County Data, (iii) use commercially reasonable efforts to prevent unauthorized access to or use of C3 Services, and notify C3 AI promptly of any such unauthorized access or use, (iv) use C3 Services only in accordance with this Agreement, Documentation, Order Forms and applicable laws and government regulations, and (v) be solely responsible for procuring County's own GitHub or similar code repository and the business intelligence tools, and for complying with terms of service of any Third Party Offering with which County uses C3 Services.

4.4. **Restrictions**. County will not, nor permit third parties to: (a) make any C3 Service available to, or use any C3 Service for the benefit of, anyone other than County, unless expressly stated otherwise in an Order Form or the Documentation, (b) sell, resell, license, sublicense, distribute, make available, rent or lease any C3 Service, or include any C3 Service in a service bureau or outsourcing offering, (c) use a C3 Service to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use a C3 Service to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of any C3 Service or third-party data contained therein, (f) attempt to gain unauthorized access to any C3 Service or its related systems or networks, (g) permit direct or indirect access to or use of any C3 Service in a way that circumvents County's obligations in this Agreement, or use any of the C3 Services to access or use any of C3 AI's Intellectual Property except as permitted under this Agreement, an Order Form, or the Documentation, (h) copy a C3 Service or any part, feature, function or user interface thereof, (i) frame or mirror any part of any C3 Service, other than framing on County's own intranets or otherwise for County's own internal business purposes or as permitted in the Documentation, (j) access, use or copy any C3 Service in order to build a competitive product or service or to benchmark with any third party product or service, (k) reverse engineer any C3 Service (to the extent such restriction is permitted by law), or (l) alter, modify or create derivative works of any C3 Services

5. NON-C3 AI PROVIDERS

5.1. **Third Party Offerings**. Any acquisition or use by County of a Third Party Offering and any exchange of data between County and any third party or the Third Party Offering is solely between County and the applicable third party. C3 AI does not warrant or support Third Party Offerings, unless expressly provided otherwise in an Order Form.

5.2. **County Data**. If County chooses to use a Third Party Offering with a C3 Service, County grants C3 AI permission to allow the Third Party Offering and its provider to access County Data as required for the interoperation of that Third Party Offering with the C3 Service. C3 AI is not responsible for any disclosure, modification or deletion of County Data resulting from access by such Third Party Offering or its provider.

5.3. **Integration with Third Party Offering**. The C3 Services may contain features designed to interoperate with Third Party Offerings. To use such features, County may be required to obtain access to such Third Party Offerings from their providers,

and may be required to grant C3 AI access to County's account(s) on such Third Party Offerings. C3 AI cannot guarantee the continued availability of such C3 Service features, and may cease providing them without entitling County to any refund, credit, or other compensation, if for example and without limitation, the provider of a Third Party Offering ceases to make the Third Party Offering available for interoperation with the corresponding C3 Service features in a manner acceptable to C3 AI. County shall ensure that County and its Affiliates have all necessary rights and licenses to interoperate any Third Party Offering with any C3 Service as contemplated in this Agreement.

5.4. **Open Source Software**. In no event will County, its Affiliates or any User use any Third Party Offerings in connection with the C3 Services that include any software code licensed under the GNU GPL or AGPL or any similar "open source" or "copyleft" license that would require C3 AI to make the source code of any part of the C3 Services available to any third party.

6. DATA PROTECTION

6.1. **Protection of County Data**. C3 AI will maintain administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of County Data, as described in the Data Security Technical Specification. C3 AI will not use County Data except (a) to provide the C3 Services and to address service or technical problems, (b) as compelled by law in accordance with Section 7.4 (Compelled Disclosure) below, or (c) as County expressly permits in writing. Where County's use of the C3 Services requires the Processing (as defined in the Regulation (EU) 2016/679) by C3 AI of Personal Data (as also defined in the Regulation (EU) 2016/679) relating to data subjects in the European Economic Area, then (a) County shall notify C3 AI in writing prior to providing it any access to Personal Data; and (b) the terms of a Data Processing Addendum will be signed by the parties and will be included with each applicable Order Form, and in such event, will apply to such Processing. Contractor's personnel will also be obligated to comply with all requirements of the Criminal Justice Information Services (CJIS) Security Policy, as set forth in Exhibit D.

6.2. **Security & Compliance**. C3 AI may monitor all use of the C3 Services for security and operational purposes. C3 AI may temporarily suspend access to any C3 Service in the event a User is engaged in, or C3 AI in good faith suspects is engaged in, any unauthorized conduct (including any violation of any terms and conditions of this Agreement, any applicable law, or third party rights); provided, however, that C3 AI will use commercially reasonable efforts under the circumstances to provide County with notice and an opportunity to remedy such unauthorized conduct prior to such suspension.

7. PROPRIETARY RIGHTS AND SUBSCRIPTIONS

7.1. **C3 AI Intellectual Property Ownership and Reservation of Rights**. Except as otherwise provided herein, C3 AI and its licensors hereby retain all right, title and interest, including all Intellectual Property Rights, in and to the C3 Materials, including all derivative works, modifications, enhancements and adaptations thereto. No rights are assigned or granted to County hereunder, other than as expressly set forth herein, and no implied license or right of any kind is granted to County. County will not delete

or in any manner alter C3 AI's copyright, patent, trademark, or other proprietary notices, if any, appearing in any C3 Materials.

7.2. **County Intellectual Property Ownership**. Except as otherwise provided herein, County hereby retains all right, title and interest, including all Intellectual Property Rights, in County's Confidential Information; if applicable ("**County Materials**"). C3 AI will not delete or in any manner alter the copyright, trademark, and other proprietary notices of County, if any, appearing on any County Materials.

7.3. **License to C3 AI**. County hereby grants to C3 AI, and shall procure the grant of, a worldwide, royalty-free, non-exclusive, non-transferable license (and, where relevant, with the right for C3 AI to sub-license to its Affiliates or subcontractors) during the term of the applicable Order Form to use, run, copy, modify, enhance, host and maintain the County Materials, and to permit is Affiliates and subcontractors to run, copy, modify, enhance, host and maintain the County Materials, in each case as necessary to perform its obligations under this Agreement and relevant Order Forms.

7.4. **County Data.** County owns all rights, title, and interest in County Data. County grants C3 AI, C3 AI's Affiliates, and applicable contractors a worldwide, limited-term license (a) to copy, transmit, display and use County Data as reasonably necessary for C3 AI to provide the C3 Services in accordance with this Agreement, and (b) to use County Data for purposes of calculating benchmarks and other analyses that C3 AI uses internally or to improve the C3 Services, provided that such use shall be solely on an anonymized basis, and C3 AI shall not use or disclose any personally identifiable information or personal data or reveal County's identity in connection with such use of County Data. Subject to the express terms herein, C3 AI acquires no right, title, or interest from County or County's licensors under this Agreement in or to any of County Data. Any additional requests from C3 AI to use County Data, including anonymized data, for purposes not expressly described in this agreement must be submitted in writing and request the written approval of the Sheriff's Office.

7.5. **License to Use Feedback**. County grants to C3 AI and its Affiliates a non-exclusive, worldwide, perpetual, irrevocable, sub-licensable, royalty-free license, without restriction, to use in any manner and incorporate into C3 AI's and/or its Affiliates' products or services, any suggestion, enhancement request, recommendation, correction, or other feedback provided by County or Users concerning C3 AI's or its Affiliates' current or future products or services ("**Feedback**").

8. CONFIDENTIALITY

8.1. **Definition of Confidential Information**. "**Confidential Information**" means all information disclosed by a party ("**Disclosing Party**") to the other party or its Affiliates ("**Receiving Party**") that is designated in writing as confidential. Regardless of marking: (a) County's Confidential Information includes County Data; (b) C3 AI's Confidential Information includes the C3 Services, C3 Materials (including C3 AI training materials), and any performance testing or benchmarking results or other evaluations of or conclusions concerning the C3 Materials; and, (c) Confidential Information of each party includes the terms and conditions of this Agreement and all Order Forms (including pricing). Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any

obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party without the use of the Disclosing Party's Confidential Information. Confidential Information also includes any information that has been made available to the Disclosing Party by third parties that the Disclosing Party is obligated to keep confidential, whether provided to the County directly or indirectly.

8.2. **Non-Disclosure**. The Receiving Party (i) will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care); (ii) will not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement; and (iii) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and permitted subcontractors and who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections not materially less protective of the Confidential Information than those herein.

8.3. **Residual Information**. C3 AI and its personnel may use any Residual Information acquired during performance under this Agreement. "Residual Information" means the ideas, know-how, and techniques retained in the unaided memories of C3 AI's personnel who have had access to County's Confidential Information in the course of performing the services under this Agreement. Either party may disclose the terms of this Agreement or any Order Form to its legal counsel and accountants without the other party's prior written consent, provided that such recipient is subject to terms of confidentiality no less restrictive than those set forth herein and the party that makes any such disclosure remains responsible for such recipient's compliance with this "Confidentiality" section. Notwithstanding the foregoing, C3 AI may disclose the terms of this Agreement and any applicable Order Form to a subcontractor to the extent necessary to perform C3 AI's obligations to County under this Agreement, under terms of confidentiality materially as protective as set forth herein.

8.4. **Compelled Disclosure**. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so. In such case, the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to that Confidential Information.

9. REPRESENTATIONS, WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS

9.1. **C3 AI Warranties**. C3 AI warrants that during an applicable Subscription Term (a) the Data Security Technical Specification will accurately describe the applicable administrative, physical, and technical safeguards for protection of the security,

confidentiality and integrity of County Data, (b) C3 AI will not materially decrease the overall security of the Subscribed C3 Applications, as applicable, (c) the C3 Applications will perform materially in accordance with the applicable Documentation, and (d) the C3 Implementation Services will be performed in a professional and workmanlike manner in conformance with generally accepted industry standards and the C3 Support Services will be performed in material conformance with Annex C-1. For any breach of a warranty above, County's exclusive remedies are as follows: (i) Section 8.1(a) above, the update of the Data Security Technical Specification to accurately reflect the applicable safeguards; (ii) Sections 8.2(b) and 8.2(c) above, the repair or replacement of the applicable functionality in the C3 Application; and (iii) Section 8.2(d), the re-performance of any substandard C3 Implementation Services or C3 Support Services, reported to C3 AI within 60 days of completion of the applicable service. The foregoing warranties are subject to County's implementation within no more than ninety (90) days of all updates and upgrades made available by C3 AI.

9.2. **Disclaimers**. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY, NOR THEIR RESPECTIVE AFFILIATES OR LICENSORS, MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY, AND THEIR RESPECTIVE AFFILIATES AND LICENSORS, SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. BETA SERVICES ARE PROVIDED "AS IS," EXCLUSIVE OF ANY WARRANTY WHATSOEVER. EACH PARTY DISCLAIMS ALL LIABILITY AND INDEMNIFICATION OBLIGATIONS FOR ANY HARM OR DAMAGES CAUSED BY THE HOSTING SERVICES OR ANY THIRD-PARTY HOSTING SERVICE PROVIDERS.

10. POST- TERMINATION MATTERS

10.1. **County Data Portability and Deletion**. Upon request by County made within 90 days after the effective date of termination or expiration of this Agreement, C3 AI will make County Data available to County in the then current format in which it was stored. After such 90-day period, C3 AI will have no obligation to maintain or provide County any of County Data, and as provided in the Documentation, C3 AI will thereafter delete or destroy all copies thereof in C3 AI's systems or otherwise in C3 AI's possession or control, unless legally prohibited.

10.2. **Surviving Provisions**. This section will survive any termination or expiration of this Agreement. Upon termination of this Agreement, the provisions of this Agreement concerning the ongoing interests of the Parties shall continue and survive in full force and effect.

11. GENERAL PROVISIONS

11.1. **Export Compliance**. The C3 Services, other technology C3 AI makes available, and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Each party represents that it is not named on any U.S. government denied-party list. County shall not and shall not permit Users to access

or use any C3 Service in a U.S. embargoed country (currently Cuba, Iran, North Korea, Sudan, Syria or Crimea) or in violation of any export law or regulation of the United States or of any other applicable jurisdiction. County will not provide to C3 AI, absent prior written notice, any data or other item that requires C3 AI to seek an export license or authorization from any United States agencies having jurisdiction.

11.2. **Anti-Corruption**. County agrees that County has not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of C3 AI's employees or agents in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction. If County learns of any violation of the above restriction, County will use reasonable efforts to promptly notify C3 AI's Legal Department at c3legal@c3.ai.

11.3. **Entire Agreement and Order of Precedence**. This Agreement, including any related Order Forms and Statements of Work constitute the entire agreement between County and C3 AI regarding County's use of the C3 Services and supersedes all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning its subject matter. Except as otherwise provided herein, no modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by the party against whom the modification, amendment or waiver is to be asserted. The parties agree that any term or condition stated in County's purchase order or in any other of County's order documentation (excluding Order Forms) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Order Form (including any exhibits), and (2) this Agreement.

11.4. **Relationship of the Parties**. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

11.5. **Waiver**. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right.

11.6. **Severability**. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

Annex C-1 -- C3 Support Services

Provided that the County ("Customer") remains current in its payment obligations to C3 AI, C3 AI will provide C3 Support Services relating to the access and operation of the C3 Materials as set forth in the table and notes below. To receive such support, Customer must report technical issues in sufficient detail and in a timely manner to C3 AI's designated support contact(s) by logging a ticket in Zendesk ("Report") and must provide assistance as requested by C3 AI to diagnose and resolve such issues. C3 AI's obligations to provide support are subject to Customer's implementation within no more than 90 days of all updates and upgrades that C3 AI makes available to Customer or generally.

Support Category	**Provision**
Case Limit	No Limit
Response Time	Response Time is measured from receipt of the Report. See Response Time Matrix[1]
On-line Self-Service Portal	Included
Support Hours	9 hours per day; 5 days per week[2]

Note 1: Response Time Matrix

Severity Level	Severity Definition	Examples	Response Time
P1	Severe Business Impact	• Production system down or not accessible • Data loss/corruption • Repeated service interruptions • Severe performance degradation impacting business	60 minutes

P2	Significant Loss of Functionality	• Critical previously available functionality missing without workarounds but system is otherwise up • Intermittent service interruptions • Noticeable but tolerable performance degradation	8 hours
P3	Minor Impact	• Some functionality not working as expected but there are workarounds available • How-to or usage questions	1 business day
P4	No Operational Impact	• Enhancement requests • General questions	3 business days

Note 2. Support Hours

Support hours for P1 are 24/7 (excluding holidays). Support hours for P2 and P3 are from 9 a.m. to 6 p.m. Pacific Standard Time excluding weekends and company holidays. C3 AI will use reasonable efforts to meet the "response time" goals set forth in the table above, based upon the aforementioned hours of operation.

Annex C2 - Service Level Agreement

1. C3 OFFERING AVAILABILITY PROVISIONS

Customer shall have the right to the availability provisions set forth herein for the Subscribed C3 Applications ("**C3 Offering**"). C3 AI's obligations set forth in this Exhibit are subject to Customer's implementation within no more than 90 days of all updates and upgrades that C3 AI makes available to Customer or generally.

2. DEFINITION OF AVAILABILITY

"**Availability**" or "**Available**" means Customer is able to access the C3 Offering via the C3 AI site. "**Downtime**" means any sustained period of time during which the C3 Offering is not Available, with the following exceptions:

2.1 Scheduled or planned maintenance (which is limited to a planned maintenance window agreed to by C3 AI and the Customer) and emergency maintenance (for which C3 AI will use commercially reasonable efforts to provide a 24-hour notice, if feasible);

2.2 Any period in which Customer is unable to use the C3 Offering due to Customer's misconduct or misuse; and

2.3 To the extent arising out of the following circumstances outside of the control of C3 AI or its third party providers:

a. a failure or malfunction resulting from scripts, data, applications, algorithms, equipment, or services provided and/or performed by Customer;

b. outages initiated by C3 AI or its third party provider at the request or direction of Customer for maintenance, back up, or other purposes;

c. outages occurring as a result of any actions or omissions taken by C3 AI or its third party providers at the request or direction of Customer;

d. outages resulting from Customer's equipment and/or third party equipment not within the control of C3 AI or its third party providers;

e. events resulting from an interruption or shut down of the C3 Offering due to circumstances reasonably believed by C3 AI or its third party providers to be a significant threat to the normal operation of the C3 Offering, the facility from which the C3 Offering is provided, or access to or integrity of Customer's Data (e.g., a hacker or a virus attack);

f. outages due to system administration, commands, file transfers performed by Customer's representatives;

g. "**Force Majeure Event**" meaning any material event or circumstance, or combination of material events or circumstances, that (a) arises after the Effective Date, (b) is beyond the commercially reasonable control of the party claiming the Force Majeure Event, (c) is not the result of the negligence of, or caused by, the party claiming the Force Majeure Event, and (d) is unavoidable or could not be prevented or overcome by the reasonable efforts and due diligence of the party claiming the Force Majeure Event, including without limitation an act of God, act of government, flood, fire, earthquake, civil unrest, act of terror, pandemic. Declared health emergency, strike or other labor problem (other than one involving the affected party's own employees), but does not include (w) nonperformance by C3 AI's suppliers, except for non-performance caused by a Force Majeure event; (x) any delay preventable by C3 AI by moving the affected services to an alternate facility; (y) changes in cost or availability of services; and (z) changes in market conditions, and provided that Customer shall not be required to pay for any services not delivered due to a Force Majeure Event; and

h. lack of availability or untimely response time of Customer to respond to incidents that require Customer's participation for source identification and/or resolution, including meeting Customer's responsibilities for any services.

3. TARGET C3 OFFERING AVAILABILITY

The "**Target C3 Offering Availability Level**" is the C3 Offering Availability Level that C3 AI plans to meet or exceed during each calendar year for which Customer is current in its payment obligations to C3 AI. The "**C3 Offering Availability Level**" is the number of hours during a particular period (as specified in the following sentence) that the C3 Offering was Available to Customer, excluding Downtime events (as defined above), divided by the total number of hours during such period (as measured at the end of such period). The Target C3 Offering Availability Level is 99.5% for the C3 Applications in any calendar year.

4. SERVICE LEVEL CREDIT

If: (a) a Downtime event occurs; (b) within seventy-two (72) hours of such Downtime event, Customer logs a service request providing detail regarding the Downtime event and requesting a Credit (as defined below), and (c) the C3 Offering Availability Level is below the applicable Target C3 Offering Availability Level as measured for the applicable period, C3 AI will issue to Customer a Credit calculated as set forth in this Section. A "**Credit**" will be equal to $1,000 for each single Downtime event with duration greater than or equal to fifteen (15) consecutive minutes and shorter than or equal to one (1) hour. If a Downtime event continues for longer than one (1) hour, Customer will be entitled to one (1) Credit for each additional consecutive hour of such Downtime event, up to the Maximum Credits. The "**Maximum Credits**" shall be a total of twenty-five (25) Credits per C3 Application in any calendar year. Customer will not be eligible to receive multiple Credits for the same service request, for multiple service requests across different C3 Offerings that arise from the same outage, or as a result of multiple service failures or outages occurring during the same period of time. Credits can be applied by Customer only towards fees owed C3 AI on a prospective basis and limited to fees due within the Term. Any Credits that remain unused at the end of the Term shall be forfeited. C3 AI shall keep track of the number of Credits accrued by Customer for each C3 Offering. Within ten (10) days after the end of each year during the term of the Agreement, C3 AI shall notify Customer of the aggregate

number of Credits accrued during the immediately preceding year for each C3 Offering, and C3 AI shall apply such Credits towards the subscription fees owed to C3 AI for the respective C3 Offering. If C3 AI meets or exceeds the applicable Target C3 Offering Availability Level for an application in a calendar year, Customer shall have no right to obtain Credit(s) for that application in the same calendar year. The remedies set forth in this Exhibit shall be Customer's sole and exclusive remedy and C3 AI's sole liability for breach of uptime obligations related to Subscribed C3 Offering.

Annex C-3 – Operational Controls

Operational Controls.

This Operational Control Section details the roles and responsibilities of the County ("Customer") and C3 AI in the deployment of, as applicable, the C3 AI Suite, C3 AI Applications, and Customer-Developed Applications, if any.

Deployment Models
Deployment of software will be Customer Cloud-Hosted. In a Customer Cloud-Hosted deployment, the software will be hosted by Customer in a Customer-managed cloud hosting services account with a third-party cloud-hosting vendor (e.g., Microsoft Azure, Google Cloud, AWS).

C3 AI and Customer Responsibilities
C3 AI's and Customer's respective responsibilities in each of the deployment models is set forth in the following RACI matrices. By way of background, a RACI matrix indicates responsibility, accountability, consultation, and information (RACI) by deployment type and task, as follows:

RACI:
R – Identifies the group responsible for completing the task or deliverable.
A – Identifies the group accountable for ensuring that the task or deliverable is completed by the responsible party.
C – Identifies the group consulted by the responsible or accountable party to determine how the task or deliverable is to be completed.
I – Identifies the group informed about the progress and completion of the task or deliverable.

The RACI matrix for each of the deployment models is set forth below and Customer shall comply with the RACI applicable to the deployment environment set forth in the applicable Order Form or Statement of Work.

Customer Cloud-Hosted Deployment
In the event that the C3 AI Suite, C3 AI Applications, and Customer-Developed Applications, if any, are deployed in a Customer-managed cloud-hosted environment, the following conditions apply:

- Customer is required to create a virtual private cloud in a dedicated C3 AI-specific sub-account to which C3 AI is provided administrative access.
- Customer is required to provide hardware (compute, storage) and networking infrastructure to meet initial and on-going License Agreement requirements of operating the C3 AI Suite and C3 AI Applications.
- C3 AI manages and operates the infrastructure, backup, incident management, provisioning, patches, and upgrades of the C3 AI Suite and C3 AI Applications.
- C3 AI monitors all components of the C3 AI Suite and C3 AI Applications through its centralized monitoring solution to help optimize and tune the C3 AI Suite and C3 AI Applications. The C3 AI centralized monitoring component resides in the C3 AI cloud environment and may be necessary for the C3 AI Suite and C3 AI Applications to function.
- Customer must provide network access to C3 AI and content providers to enable continuous

content updates (e.g. weather, geospatial, documentation).

The following RACI[1] matrix indicates responsibility, accountability, consultation, and information (RACI) by deployment type and summarizes the customer and C3 AI responsibilities in a Customer Cloud-Hosted deployment.

	C3 AI Operations	C3 AI Support	Customer	C3 AI Access level Req'd
Infrastructure as a Service	C, I	C, I	R, A	Admin level Access
C3 AI Suite				
Provisioning	R, A	I	I	Cluster Admin
Patches & Upgrades	R, A	I	C,I	Cluster Admin
Backup & Restoration	R, A	I		Infrastructure Admin
Incident Management	R, A	I	I	Infrastructure Admin
Infrastructure Monitoring	R, A	I	I	Infrastructure Admin
System Performance Monitoring	R, A	I	I	Infrastructure Admin
System Availability Monitoring	R, A	I	I	Infrastructure Admin
System and Data Security Monitoring	R, A	I	R, I	Infrastructure Admin
C3 Applications				
System and Performance Monitoring	R, A	C, I	I	Cluster Admin
Incident Management	R, A	C, I	C, I	Cluster Admin
Provisioning	R	A, C	I	Cluster Admin
Patches & Upgrades	R	A, C	I	Cluster Admin
Customer Developed and C3 Extended Applications				
Performance Monitoring	C, I	C, I	R, A	None
Incident Management	C, I	C, I	R, A	None
Provisioning	C, I	C, I	R, A	None
Patches & Upgrades	C, I	C, I	R,	None

[1] **RACI:**
R – Identifies the group responsible for completing the task or deliverable.
A – Identifies the group accountable for ensuring that the task or deliverable is completed by the responsible party.
C – Identifies the group consulted by the responsible or accountable party to determine how the task or deliverable is to be completed.
I – Identifies the group informed about the progress and completion of the task or deliverable.

			A	
App Admin (e.g., user & content management)			R, A	
Data Classification & Access Control		I	R, A	

	C3 Responsibility	Customer Responsibility
C3 AI Suite		
Infrastructure	C3 AI is responsible for: • Communicating infrastructure, hardware, network, and storage requirements • AMIs, Virtual Images, or Docker containers for the C3 AI Suite and related software components	Customers are responsible for: • Infrastructure virtualization and hardware per C3 AI specifications • Network/subnet configuration per C3 AI specifications • Operating system patches • A file system that C3 AI can use for file storage. For AWS deployments, S3 is used as the file system. For Azure deployments Blob storage is used as the file system. • Providing C3 AI secure administrative access to the Customer environment
C3 AI Suite Installation and Configuration	C3 AI is responsible for the installation and configuration of the C3 AI Suite and related softwarecomponents.	
Upgrades and Patches	C3 AI targets quarterly releases of the C3 AI Suite. C3 AI may also need to apply patches out of cycle to correct or prevent critical system issues. Patching and upgrades are performed on the C3 AI Suite and related software. Patches and/or upgrades that impact the availability of applications will be coordinated with the primary Customer contact.	
Infrastructure Monitoring	C3 AI provides 24x7 system monitoring. Monitoringof the C3 AI Suite includes system availability and capacity monitoring.	
Backup and Restoration	Daily backups of data stores including: the key value store, relational, and multi-dimensional data stores.	

Incident Management	C3 employs a dedicated team of technical experts to deliver proactive and preventative maintenance. Incident tickets areused to track and assign priority and severity to all incidents.	
C3 Applications		
Provisioning	C3 AI is responsible for the provisioning of C3 AI Applications.	

	C3 Responsibility	Customer Responsibility
Patching and Upgrades	C3 AI targets quarterly releases of the C3 AI Applications. C3 AI may also need to apply patches out of cycle to correct or prevent critical system issues. Patches and/or upgrades that impact the availability of applications will be coordinated with the primary customer contact.	
Monitoring	C3 AI provides 24x7 system monitoring for applications it manages on the behalf of its customers. Monitoring of C3 AI Applications includes: • Application availability • Data loading and remediation of any data load failures • Work queue monitoring	Customer provides access to C3 AI's cloud monitoringenvironment hosted and managed in a C3 AI account.
Incident Management	C3 AI employs a dedicated team of technical experts to deliver proactive and preventive maintenance. Incident tickets are used to track and assign priority and severity of all incidents.	
Customer Developed and C3 Extended Applications		
Provisioning		Customer is responsible for the provisioning of applications they develop or C3 AI applications that they have extended.
Patching and Upgrades		Customer is responsible for managing and coordinatingtheir application upgrades and patch releases.

Monitoring		Customer is responsible for the monitoring of applications they develop and deploy on the C3 AI Suite. Monitoring of C3 Applications includes but is not limited to: • Application availability • Application response time • Data load activities and remediation of any data load failures • \Work queue management
Incident Management		Customer is responsible for the tracking and resolution ofissues and incidents for the applications they develop or the C3 AI Applications they extend.
App Admin (e.g., user management, content admin)		Customer is responsible for the management andadministration of: • Application users (app users, developers, and administrators) • Application security configuration (permissions, roles, admin groups)
Data Classification and Access Control		Customer is accountable to ensure their solution and its data are securely identified, labeled, and correctly classified to meet any compliance obligation. Distinguishing between sensitive customer data and content designed to be private or personally identifiable must be done by Customer. Customer's accountability for data classification and management should be acknowledged as an essential part ofthe planning process. In such solutions, Customer needs to configure and establish process to protect both the data and the solution's feature set that protects their data.

Exhibit D

California Department of Justice and County of San Mateo Data Security Policies

1. C3 shall provide a list of its employees that require access to the County's system and data pursuant to the Agreement. The list shall be updated and provided to the Departments and the County's Chief Information Officer (CIO) or his/her designee within 24 hours of staff changes.

2. C3 and the County will jointly complete the US DOJ Cloud Requirements matrix, network diagram, and application forms for DOJ approval of the production environment.

3. C3 agrees to comply with US Department of Justice (DOJ) Criminal Justice Information Services (CJIS) Security policy v5-9 (06/01/2020), the CLETS Private Contractor Management Control Agreement, and the County of San Mateo Vendor/Contractor Access Policy (updated as of October 22, 2018).

Exhibit E

C3 AI Suite™

Technical Specification C3001: C3 AI Suite, Applications, and Data Security

Policy Title		Policy Type
C3001: C3 AI Suite, Applications, and Data Security		Information Technology
Policy Cross Reference	Version No.	Version Date
NA	1.8	October 2021
Approval Signoffs		
Name and Title		**Signature**
Ed Abbo, President and Chief Technical Officer		N/A
Houman Behzadi, Chief Product Officer		
Ali Zahabi, Vice President Operations & IT		
Last reviewed		October 2021

Revision History

Revision date	Items revised	Author	Approved Version
20-July-2017	Initial version	Scott Kurinskas	v1.0
December 2017	Added confidentiality requirements regarding ePHI	Ali Zahabi	v1.1
July 2018	Modified file name due to browser compatibly issue. Included language for general public cloud providers.	Ali Zahabi	v1.2
September 2018	Modified defined terms to conform	Ali Zahabi	v1.3
October 2018	Replaced references to C3 IoT with C3	Kira Kimhi	v1.4
September 2019	Replaced Platform with AI Suite	Ali Zahabi	V1.5
September 2020	Modified Secure Code Development Process	Ali Zahabi	v1.6
August 2021	Reviewed and Updated C3.ai logo	Ali Zahabi	v1.7
October 2021	Updated data encryption section	Ken Okumura	v1.8

Table of Contents

A. C3 SECURITY

A.1. INTRODUCTION

The C3 AI Suite™ and C3 Applications employ advanced analytics and machine learning at scale to deliver real-time or near real-time actionable insights for enterprise business imperatives.

C3 understands that the security, confidentiality, integrity, and availability of the C3 AI Suite™ and the C3 Applications are important to customers. C3 delivers a unified, cohesive suite of products through a scalable and secure hosting model:

- C3 products are delivered as hosted PaaS and SaaS offerings deployed in secure Virtual Private Clouds. This provides system scalability and data security combined with low overall cost of ownership.

- C3 implements a rigorous Cyber Security Program to protect critical systems and information assets, constantly monitoring and improving applications, systems, and processes to meet the growing demands and challenges of security.

Security of C3's hosting operations and C3 AI Suite™ has been validated in production deployments for leading utility operators and large commercial and industrial organizations around the world.

A.1.1. C3 Cyber Security Program

The C3 Cyber Security Program is a multi-layered security approach that employs technical, physical, and administrative safeguards.

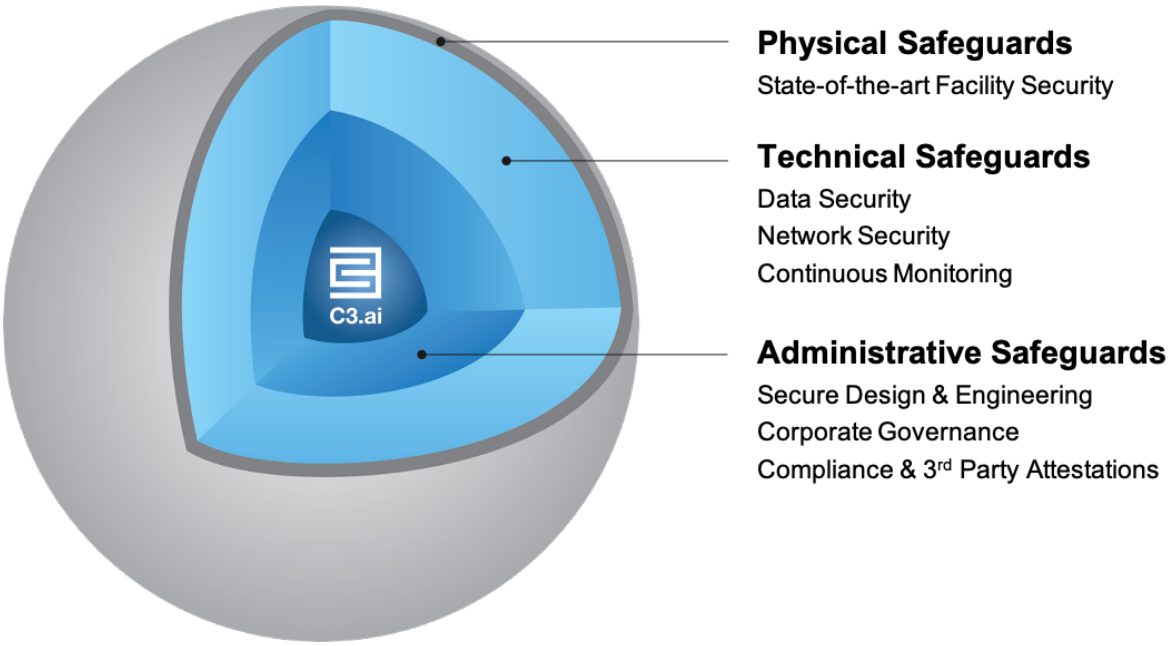


Figure 1: C3 AI Cyber Security Program's multi-layered security approach.

The C3 Cyber Security Program has been developed to comply with the applicable legal and regulatory requirements, including compliance with the NERC CIP smart grid cyber security standards. This program encompasses a comprehensive set of cyber security controls and business processes based on NIST best practices that align with the NERC CIP standards.

Physical Safeguards

- ***Physical and Operational Security:*** C3 combines state-of-the-art data center facilities with industry best practices to ensure operational security. A detailed description of C3's physical and operational security follows in Section A.2.

Technical Safeguards

- ***Network Security:*** C3 provides Virtual Private Clouds accessible over robust network infrastructure to provide secure and reliable systems. A detailed description of C3's network security follows in Section A.3.

- ***Data Security:*** Data security is a fundamental requirement that is systematically addressed throughout the C3 AI Suite™. This includes access controls, encryption, user roles, and data retention/destruction A detailed description of C3's data security follows in Section A.4.

- ***Continuous Monitoring:*** C3 uses multiple, redundant, continuous monitoring systems application and data security. A detailed description of C3's continuous monitoring follows in Section A.5.

- ***Business Continuity:*** C3 backup, failover, and redundancy services ensure data availability and protect information from loss or destruction. A detailed description of C3's business continuity measures follows in Section A.7.

Administrative Safeguards

- ***Secure Design and Engineering Principles:*** C3 follows best practice secure software development processes to incorporate security throughout the product development and release lifecycle. A detailed description of C3's design and engineering methodologies follows in Section A.6.

- ***Corporate Governance:*** Cyber security is a strategic priority for C3. C3 has implemented extensive corporate oversight to ensure its ongoing success. A detailed description of C3's cyber security corporate governance follows in Section A.9.

- ***Third-Party Attestations:*** C3 offers a variety of third-party attestations regarding cyber security processes and controls.
    - C3 undergoes regular testing by external security experts, including source code reviews, software vulnerability testing, and penetration testing.
    - C3 uses data centers that have been audited for the leading industry IT security standards, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), SOC 2, FISMA, DIACAP, FedRAMP, PCI DSS Level 1, ISO 27001, International Traffic in Arms Regulations (ITAR), and FIPS 140-2.

  A detailed description of C3's third-party attestations follows in Section A.10.

A.2. PHYSICAL AND OPERATIONAL SECURITY

A.2.1. Data Center Operations

C3's customer systems infrastructure is hosted at well-established cloud data centers like Amazon AWS, Microsoft Azure and Google GPC in Northern Virginia, Oregon, and Dublin Ireland depending on data jurisdiction. These data centers represent that they provide best practice security and reliability features, including secure premises with video surveillance, power supply & backup, precision environmental controls, equipment monitoring, comprehensive security policies & controls, and third-party security compliance and attestation, as described below.

Secure premises – Facilities are nondescript and unmarked to help maintain a low profile. All visitors must pass through a security check-in before accessing the facility. Biometric scanning controls data center access, and access is available only to data center personnel and contractors who have a legitimate business need for such privileges. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Data center access is logged and monitored. 24x7 onsite staff provide additional protection against unauthorized entry. CCTV camera monitoring is present at all data center locations. Audit logs for sensitive areas are maintained and reviewed regularly.

Power supply and backup – Multiple levels of built-in power redundancy provide a high level of availability. Generators and Uninterrupted Power Supply (UPS) provide backup power sources and prevent power spikes, surges, and brownouts. If a total utility power outage ever occurs, these power systems are designed to ensure that the data centers will continue to operate. The UPS power subsystem is N+1 redundant, with instantaneous failover if the primary UPS fails. If an extended utility power outage occurs, on-site generators can run indefinitely. All on-site generators are tested regularly.

Precision environment – Heating, ventilation, and air conditioning (HVAC) systems provide appropriate and consistent airflow, temperature, and humidity levels. Every data center's HVAC system is N+1 redundant. This ensures that a duplicate system immediately comes online should there be an HVAC system failure. Advanced fire suppression systems are designed to stop fires from spreading in the unlikely event one should occur.

Equipment monitoring – All electrical, mechanical, and life support systems and equipment are monitored to ensure that any equipment issues are immediately identified. Preventative maintenance is performed to maintain continuous operability of all equipment.

Third-party compliance and attestation – The data centers are designed and managed in alignment with security best practices and a variety of established IT standards, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), SOC 2, FISMA, DIACAP, FedRAMP, PCI DSS Level 1, ISO 27001, International Traffic in Arms Regulations (ITAR), and FIPS 140-2.

A.2.2. C3 Corporate Processes

Policies – C3's Executive Management has instituted a set of policies, procedures, and guidelines to ensure the security of the C3 AI Suite™ and C3 Applications. These policies apply to all employees. In cases where additional policies and procedures have been called out, these additional policies and procedures apply to employees with access to designated customer projects with access to sensitive data.

Corporate security – C3 maintains stringent physical security at all offices. Each person with authorized access is provided an electronic key to gain entry and move within the facilities. All visitors are required to sign-in and to be escorted by authorized staff.

Background checks – Background checks, as permitted by law, are mandatory for all employees and contractors. These include, as permitted by law, criminal checks, education and employment verification, and reference checks. Drug testing may be performed for designated customer projects.

Proprietary information – All employees and contractors are required to sign a Proprietary Information Agreement as a condition of employment. All subcontractor agreements include rigorous confidentiality and non-disclosure clauses.

Security awareness program – All C3 employees are trained on C3's security policies upon initial hiring and on an annual basis.

Employee access – Formal procedures govern user accounts for all employees. They regulate user roles and access, as well as the ability to add, delete, and modify user accounts. The C3 Human Resources (HR) department provides an immediate alert to the C3 Operations team when an employee has had a change in functional role or has been terminated. C3 Operations then modifies or disables system/network/e-mail access as per the HR alerts upon notification. Privileged user accounts are controlled and reviewed every 60 days.

Asset management – An inventory is kept of all hardware, software, and intellectual property assets. This inventory documents permitted configurations, usage, and access, along with other applicable controls.

Workstation protection – Anti-virus software is installed on all Microsoft Windows workstations (with daily virus signature updates). Preventative controls, such as screen timeout (5 minutes of inactivity) and session timeouts (configured on a per application basis), are required to prevent unauthorized access to unattended systems. Confidential corporate information stored on workstations must be encrypted. Confidential information is not permitted on removable media.

Use of USB enabled removable storage media is enabled on a need-to-have basis. If business needs dictate the use of USB enabled removable storage media, technical security controls are put in place (company owned devices only, device encryption) to ensure sensitive data is secured on a USB device. For employees that have access to sensitive data, USB ports are disabled.

Audits – Multiple security audits are performed regularly, including daily review of user access logs, quarterly review of user access rights and asset policies.

A.3. NETWORK SECURITY

C3 applies security best practices to a state-of-the-art network infrastructure to provide a secure and reliable platform.

A.3.1. Data Communication

C3's data centers maintain redundant relationships with multiple Internet Service Providers, and employ robust routing using the BGP4 networking protocol to allow network traffic to take the best path. All customer data in transit (network connections to C3) is securely transmitted using HTTPS (SSL/TLS) with 4096-bit RSA encryption.

A.3.2. Secure Network Architecture

The C3 network architecture is designed to maximize security, scalability, and reliability.

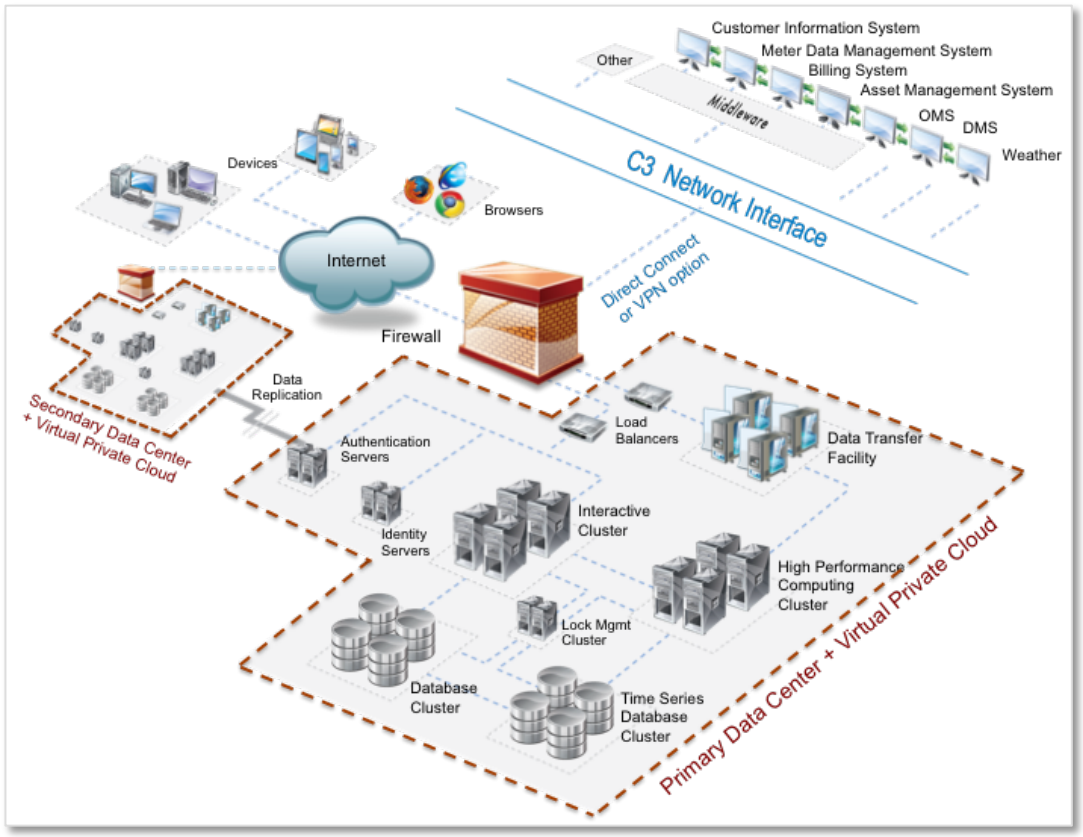


Figure 2: The C3 Network Architecture

Network access to and from C3 customer system infrastructure is controlled by network devices (including firewalls), switching access control lists, and load balancing. These boundary devices employ rule sets, access control lists, and configurations to enforce and monitor the flow of information to the C3 servers.

Firewalls and ports – Multiple network devices provide traffic filtering services. The only open inbound ports and protocols are HTTP, HTTPS, and SMTP. All other ports and protocols are explicitly disabled, thereby preventing worms and other network-based attacks.

Bastion servers – Bastion servers provide secure connectivity services deployed within customer-dedicated Virtual Private Clouds. Bastion servers are configured with all unnecessary services, protocols, programs, and network ports disabled to minimize the risk of unauthorized users gaining privileged access to customer-dedicated Virtual Private Clouds. Additionally, Bastion hosts are configured with security groups to provide fine-grained ingress control.

Reverse proxies – Load balancers serve as reverse proxies, distributing system load while further protecting C3 application servers from direct access.

Two-factor authentication – Access to C3 servers requires use of a Virtual Private Network with multi-factor authentication and access monitoring.

Hardening standards – C3 follows the National Security Agency's (NSA) recommended hardening standards for all deployed server instances. These hardening standards are applied at server instantiation and reviewed monthly.

OS upgrades and patches – Operating system patches are reviewed upon release. Depending on the assessed priority and risk, operating system patches and upgrades are scheduled for implementation in accordance with industry best practices.

Virtual Private Cloud – C3 offers customer-dedicated Virtual Private Clouds. Each Virtual Private Cloud is a private network subnet that isolates customer server instances from any other customer's deployment. This provides uncompromising cyber security while enabling cost-effective system scalability.

Direct connect – C3 offers customers the options of Virtual Private Network (VPN) encrypted tunnels and private lines to connect to C3's data centers, thereby ensuring secure transmission along with the option to completely bypass internet service providers (public internet) in the network path.

Development, staging and production environments – C3 implements independent development, staging, and production environments for all customer deployments, thereby further protecting the security and reliability of production systems.

C3 corporate segregation – C3's internal corporate network is segregated from all customer systems, further restricting unnecessary access to production systems.

A.4. DATA SECURITY

C3 has implemented comprehensive *defense-in-depth* customer data security and protection, encompassing data access administrative controls, data encryption, user roles, and data retention / destruction.

A.4.1. Administrative Controls

Data access – Access to Customer Data is restricted to authorized personnel only, according to documented processes. Only those C3 personnel explicitly identified in an application implementation role have access to customer systems. For application implementation personnel, customer system access is promptly de-activated as soon as the implementation is complete and access is no longer necessary. Access to all servers is limited, logged, and tracked for auditing purposes.

Data security policies – Customer Data Handling and Secure Document Destruction policies are enforced for the management of all sensitive information. All C3 employees are trained on documented information security and privacy procedures. C3's Cyber Security Team performs quarterly reviews of C3 personnel who have access to customer environments and systems, to track activity and validate access.

Data and environment separation – Each C3 customer has separate databases with distinct access controls. C3 implements independent development, staging and production environments for each customer system deployment. C3's internal corporate network is segregated from all customer environments.

Data Classification - All C3 employees and contractors have been educated on the C3 data classification policy and must apply these policies in their daily C3 business activities. Sensitive information is either Confidential or Restricted information. This data classification policy is applicable to all electronic information and paper documentation for which C3 is the custodian.

All electronic information managed by C3 must have a designated owner. Owners are responsible for assigning appropriate sensitivity classifications as generally described below, subject to adjustments based on specific customer's data.

- **Restricted** — This classification applies to the most sensitive confidential business information.
- **ePHI** — This classification applies to "electronic protected health information," or ePHI according to The Health Insurance Portability and Accountability Act of 1996.
- **Confidential** — This classification applies to less sensitive confidential business information.
- **Public** —This classification applies to information that is not subject to confidentiality restrictions.

Data Owners are responsible for decisions about who will be permitted to gain access to information, and the uses to which this information will be put. C3 has policies and procedures in-place to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information as described in this document.

A.4.2. Data Encryption, Protection, and Destruction

Data encryption – C3 implements enterprise class encryption to provide added data security. Customer Data at rest is encrypted using AES-256 encryption. Any Customer Data in motion is securely transmitted using HTTPS (SSL/TLS) with 4096-bit RSA encryption.

Data protection – C3 implements comprehensive data protection and recovery measures in accordance with the following established industry best practices. Data backups are performed on a nightly basis and are replicated to a designated backup C3 data center. The backup data center is geographically separated and independent from a customer's assigned primary and secondary C3 data centers. All ePHI backup is encrypted and backup data is transferred in a secure, encrypted manner using HTTPS (SSL/TLS) with 4096-bit RSA encryption, and is securely stored in encrypted form at a backup facility. To facilitate rapid data restoration, the primary backup method is an encrypted, hardware-level replication. Backups can be restored and end-user accessible within eight hours of process initiation. Backup data restoration is tested on a monthly basis. All backup activity, including transport, storage, and access, is logged and regularly audited to ensure proper handling.

Data destruction – C3 applies data destruction measures in accordance with established industry guidelines. Standard backup Customer Data retention is 30 days, after which the backup such data is permanently destroyed. C3's Operations team permanently destroys all Customer Data at the end of the applicable contract, including then-existing customer databases and backup repositories. All Customer Data destruction is logged and regularly audited.

A.4.3. Application Security

Role-based access – C3 Application access for end-users is controlled via user roles. These roles control security and access rights for standard users, super users, and administrators.

Application access segmentation – End-user application access can also be restricted based on data values. For example, customer end-users can be granted access to only the assets, accounts, or geographic regions that are necessary for their areas of responsibility.

Network IP access – Customer's access to C3 Applications can be restricted to specific networks and locations (configurable via designated IP space whitelisting and/or blacklisting).

Single Sign On (SSO) – C3 enables customers to use their existing end-user authorization systems to manage access to the C3 Applications. C3 supports SSO integration with any version of LDAP or Active Directory that supports SAML.v2.

Login information protection – To prevent password guessing attacks, account access is automatically suspended after a configurable number of unsuccessful password entry attempts.

Configurable password parameters – Customer system administrators can configure the complexity, length, and expiration requirements of end-user application passwords to adhere to their existing corporate standards.

Configurable application session timeout – C3 Application session timeout can be configured on a per-customer basis, adhering to their existing corporate standards.

A.5. HOSTING OPERATIONS

A.5.1. Security Monitoring

C3 uses continuous monitoring methods to ensure C3 application and Customer Data security.

Application access logging – C3 tracks all C3 Application access, including failed authentication attempts, and keeps two years of historical records to support reporting and auditing requirements. All successful and unsuccessful access activities are recorded in the system and in application logs, along with username, IP address, action, and date/time of access. Every data change is logged in the system and in application logs.

Alerting – C3 is committed to frequent and transparent customer communication. The C3 Cyber Security Team monitors and alerts customers of suspicious activity including but not limited to multiple failed login attempts, abnormal usage patterns and large data access/downloads. C3 has a formal process to notify customers of a verified security breach, theft, or loss of data. High alert (Priority P1) incidents are responded to on a 24x7 basis, with all incidents tracked in a case management system.

A.6. SECURE DESIGN AND ENGINEERING

A.6.1. Scalable Architecture

The C3 AI Suite™ is the software foundation that handles data management, multi-layered analysis, and data visualization capabilities for all C3 Applications. The C3 AI Suite™ has been specifically designed to process and analyze significant volumes of frequently updated data while maintaining high performance levels.

The C3 AI Suite™ architecture is comprised of multiple services with each handling a specific data management or analysis capability. All the services are modular, and have been architected to execute their respective capabilities intended to maximize security.

A.6.2. Secure Code Development Process

C3's software development process follows the Open Web Application Security Project (OWASP) standards for building secure applications, including mandatory internal review by the C3 Cyber Security Team. The C3 software development cycle includes stringent code review, as well as integration and regression testing prior to release with internal and external testing tools to check for security vulnerabilities. Static code analysis tools are run as a part of the standard software build process, and all deployed software undergoes recurring penetration testing. All test results are shared with the C3 Engineering team and any detected issues are resolved prior to final product release.

To maintain security throughout the entire lifecycle of the C3 AI Suite™ and to prevent the injection of harmful code, security testing is performed regularly and systematically. Anti-malware is installed on endpoints to detect and disable malware and harmful code. File integrity checks are performed to ensure no unauthorized changes occur in the installed software. Secure server-side session management is implemented with detailed event logging. The C3 AI Suite employs least privilege principles and encrypts all sensitive data at rest and in transit. Quarterly SAST and DAST vulnerability scans are conducted. All third-party and open source components used in the C3 architecture are selected based on their stability and industry support, are scanned during CI/CD process, and are subject to the same security testing as any internally developed C3 code. All external components of the C3 architecture are kept current with validated software patches. All patches are reviewed and tested by the C3 Operations Team before deployment as part of C3's standard change management process. All server instances are re-imaged with hardened and tested OS, software, network, and security versions prior to deployment.

A.6.3. Security Audits

Internal vulnerability and penetration testing – The C3 Cyber Security Team performs vulnerability and penetration testing for every new C3 Application version, using open-source and commercial testing tools. A version is not released until all identified vulnerabilities are corrected and the version successfully passes security testing.

Third-Party vulnerability testing – C3 engages third-party security experts to perform annual penetration testing and security audits. These testing cycles involve source code review, software vulnerability testing, and penetration testing. Any vulnerabilities identified in these testing cycles are immediately corrected, and C3 has consistently passed security audits.

A.7. THIRD PARTY CERTIFICATIONS AND ATTESTATIONS

The C3 Cyber Security Program has been developed to comply with applicable legal and regulatory requirements, including compliance with the NERC CIP smart grid cyber security standards. This program encompasses a comprehensive set of cyber security controls and business processes based on NIST best practices that align with the NERC CIP (versions 3 and 4) standards.

To objectively verify adherence to these processes, C3 works with industry auditors that bring additional levels of scrutiny to the security of C3 Applications and the processes that govern how they are developed, tested, deployed, and supported. C3 has successfully completed multiple third-party security tests, including source code reviews, software vulnerability testing, and penetration testing.

For SaaS and PaaS offerings, C3IoT uses data centers that are regularly audited for a variety of established IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II)
- SOC 2
- FISMA
- DIACAP
- FedRAMP
- PCI DSS Level 1
- ISO 27001
- International Traffic in Arms Regulations (ITAR)
- FIPS 140-2