Gun & Incident Detection Software Response and Technical Proposal File

RFP-185-2528-2026 - IntelliSee - Technical Proposal

Submitted by: Scott Keplinger, CEO (s.keplinger@intellisee.com)

IntelliSee®

Smarter surveillance for a safer world

Section 1: Transmittal Letter

IntelliSee
Smarter surveillance for a safer world

www.intellisee.com

December 15, 2025

Thank you for the opportunity to bid on the Iowa Department of Management's RFP - 185 - 2528 - 2026: Autonomous Gun and Incident Detection & Alerting Software. We are excited to be considered for the opportunity to help improve the safety and cost profile for our state's schools and others.

Please accept this Transmittal Letter as additional attestation that IntelliSee has read, understands, and agrees with the terms and conditions of this solicitation - including all addenda and attachments hereto and that IntelliSee has read and understands the Scope of Work and the nature of the goods and services being solicited. I also attest I am authorized to bind IntelliSee to this solicitation's terms and conditions.

IntelliSee (intellisee.com), is a mission-based, early stage technology firm in Coralville, Iowa formed by Iowans to help address the dramatic rise in school violence, costs, and risks. Several Iowa-based customers, installers, investors, and partners - including the Iowa Economic Development Authority - are supporting our mission to help improve safety through our new, advanced technology.

We improve safety through our IntelliSee application that autonomously monitors customers' existing surveillance cameras with ethical AI to detect a broad and growing range of visible threats and risks. Once detected and validated, alerts inform designated people and systems - including first responders - with the situational awareness needed to ultimately prevent and reduce harm.

We started with brandished weapon detection and have similar capabilities - including human verification, 911 integration, and SAFETY Act designation - as the market leader in gun detection. However, we have expanded beyond this foundation to also detect more commonly occurring threats and risks that also drive significant harm and cost to our schools and others. This is an important distinction given organizations leveraging IntelliSee are able to add a new safety layer that helps protect them from the horrors of an active shooter event while also protecting themselves against issues that are much more likely to occur.

Because of this, we help schools and others improve safety *and* save money with a system that is comparably priced to those that only detect brandished weapons. As a mission-based company, we also continually expand our platform at no additional cost. No cost updates, upgrades, and support are all part of our effort to improve school safety with a product that continually increases in value while helping our schools manage through an increasing number of challenges.

This proposal describes all of this in more detail and is structured per the requirements of the RFP but in a format that hopefully clearly answers all questions while conveying our passion for school safety. Thank you again for the opportunity to participate and we look forward to helping keep our state safe.

Sincerely,

Scott Keplinger
IntelliSee Co-founder and Chief Executive Officer
808 5th Street, Coralville IA 52241
s.keplinger@intellisee.com
(515)783-6738

Section 2: Proposal Table of Contents

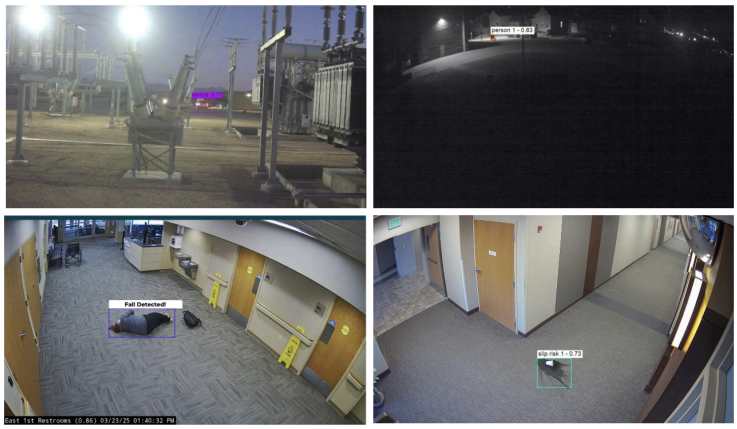
Section 3: Scope of Work & Overview

IntelliSee (intellisee.com), is a mission-based, early stage technology firm in Coralville, Iowa that formed to help address the dramatic rise in school violence, costs, and risks. Several Iowa-based customers, installers, investors, and partners - including the Iowa Economic Development Authority - are supporting our mission to help improve safety through our new, advanced technology.

IntelliSee formed to help stop school shootings by visually detecting the presence of brandished (drawn) guns - this includes handguns, long guns, assault rifles, and other types of guns. Our AI platform overlays with an organization's ***existing*** surveillance cameras (and other safety infrastructure) to actively monitor cameras and autonomously detect a broad and growing range of visible threats in real-time. Once detected and validated, alerts inform designated parties (and other systems) so they can act to prevent and mitigate harm. Our AI is deep-learning (the most advanced that mimics how the human brain learns) computer vision AI. Computer vision is a field of AI that analyzes visual data / pixel combinations to predict events.

Detecting and alerting on drawn weapons provides the critical time needed to prevent casualty events through lockdown protocols and first responder notification. IntelliSee gun detection includes 24/7/365 human verification and first responder / 911 escalation via our dedicated team of experts and partnership with RapidSOS - the pre-eminent 911 call center integration and alert monitoring service in the U.S. Geo-located alerts are sent in real / near real-time to designated parties (e.g. SRO's, administrators, etc.), to other systems (e.g., video management systems, mass notification systems, access controls, mapping systems, etc.), and first responders / 911. This enables rapid response to prevent harm and saves lives.

This risk is real and increasing however *it is* ***extremely*** ***rare***. *Most organizations - including public schools - will never suffer a shooting event.* IntelliSee's insurance partners (e.g. Holmes Murphy and others) and others indicated an ideal solution should ***also*** mitigate other costly and dangerous risks. As a result, IntelliSee's unique solution detects drawn guns ***and*** other visually detectable risks via the same system. Detectable risks / threats include trespassing, vehicles, loitering, falls, crowds, leaks, spills, cellphones, smoke / fire and new capabilities are continually added at no additional cost to customers.



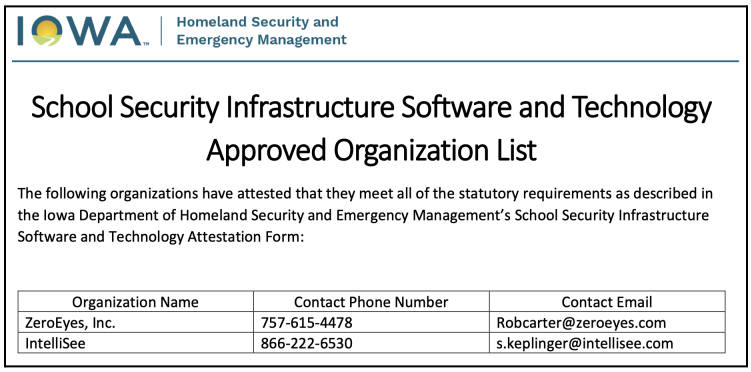
This protects organizations against rare active shooter events *while also protecting against other harmful risks / threats that occur much more frequently and that drive significant costs.* Customers *are not limited* to which capabilities they leverage so they get day-to-day value while also protecting against rare but potentially catastrophic events.

Given our mission, IntelliSee *continually adds* new capabilities - including new detection capabilities - *at no cost to users* (a significant differentiator vs. alternatives). For example, cellphone detection was released this fall and smoke/fire detection is already in beta release with current customers. Similarly, the system is easily expandable, highly flexible, and has a very customer-friendly licensing approach. Installations are quick and non-complex, we do not limit the number of users, customers can toggle cameras on/off at no additional cost, and we have a litany of options available to protect organizations regardless of size.

IntelliSee is designed as an open system to complement other existing infrastructure. Beyond integrating with nearly any type of existing surveillance camera, IntelliSee integrates with other ancillary systems, including Video Management Systems (VMS), Mass Notification Systems (MNS), Access Controls, Public Address, Mapping Systems, and others. Doing so enables organizations to leverage their existing protocols and assets/infrastructure to improve safety via the situational awareness IntelliSee provides.

IntelliSee also balances privacy with safety. No personally identifiable information (PII) is processed, stored, nor used by IntelliSee; IntelliSee does not and will not do facial recognition; no surveillance footage is stored nor transmitted; IntelliSee's hardware processes within customer firewalls; data is encrypted; we perform regular penetration tests; and we adapt our default cybersecurity to customer needs.

As a result, IntelliSee has been designated as a Department of Homeland Security Safety Act Qualified Anti-Terrorism Technology (QATT) - see www.safetyact.gov - and is listed on the Iowa Homeland Security and Emergency Management website as a School Security Infrastructure Software and Technology Approved Organization List (see graphic to the right or this link).



IOWA | Homeland Security and Emergency Management

School Security Infrastructure Software and Technology Approved Organization List

The following organizations have attested that they meet all of the statutory requirements as described in the Iowa Department of Homeland Security and Emergency Management's School Security Infrastructure Software and Technology Attestation Form:

Organization Name	Contact Phone Number	Contact Email
ZeroEyes, Inc.	757-615-4478	Robcarter@zeroeyes.com
IntelliSee	866-222-6530	s.keplinger@intellisee.com

This also reflects that IntelliSee is a U.S. company; was created in the U.S. by U.S developers; shareholders are U.S. citizens; servers reside in the U.S.; U.S. hardware is used; and that no association with any company that is owned or controlled by the People's Republic of China (or any other country) exists.

Through IntelliSee, organizations are now able to do the following using their existing cameras:

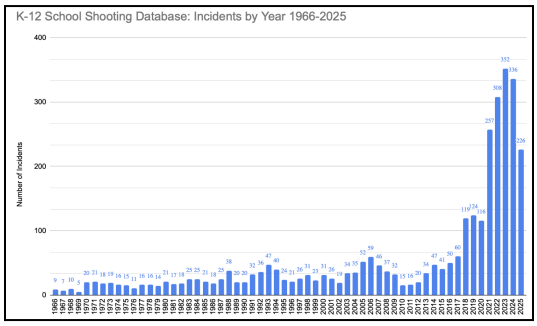
- Improve situational awareness and emergency response capabilities.
- Leverage existing surveillance systems to detect and alert on multiple threats.
- Leverage ethical, privacy-conscious AI implementation.
- Reduce reliance on manual monitoring and rule-based systems.

Technical Proposal Submission

Threat Detection and Incident Resolution

School vulnerabilities and challenges are high and getting worse as our society struggles to cope with mental health, extreme political polarization, and funding constraints. Unfortunately, economists are predicting increasing economic uncertainty which will further amplify these challenges. Consider:

- School shootings have increased dramatically and are expected to continue (link & graphic below)
- Break-ins, vandalism, and other school crimes cost schools $600million+ annually (link)
- Falls are the most frequent worker compensation claim and schools have an even higher incident rate (source)
- Insurance fraud has a $300B economic impact and ~1 in 17 fall claims are fraudulent (source)
- Solo workers (e.g. janitors) in schools greatly increase risk due to issues like medical emergencies (source)
- Most states now ban cellphones in schools and they are also a leading safety distraction (source)

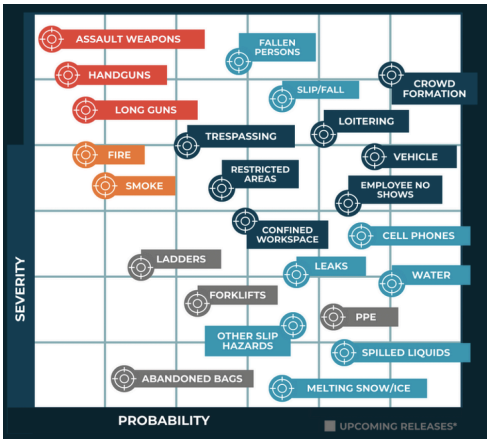


- Despite codes, ~9 schools experience fires per day with arson being the leading cause (link)

No organization - whether a public or private school, municipalities or other public organizations, private industry, non-profits, or others - is immune from these same challenges. IntelliSee is designed to help by detecting a growing range of threats & risks our public schools and others face (see below graphic).

To our knowledge, IntelliSee is the only organization that:

- Detects a range of threats all at once via a single platform:
  - Branded firearms (handguns, longguns, assault rifles)
  - Unauthorized vehicles/persons in defined zones
  - Loitering and crowds / multiple persons in zones
  - Zero occupancy in defined zones
  - Falls/persons on the ground
  - Leaks, spills or pooled liquids
  - Cellphones
  - Visible smoke & fire
  - Camera outages or transmission failures



- Continually expands the types of risks / threats detected
- Provides customer access to the entire platform for a single annual subscription cost (vs. menu-based pricing)
- Includes maintenance, updates, and upgrades within its annual fee so its value continually to grows

IntelliSee's "common to catastrophic" coverage adds a safety layer that can also save money via a combination of incident prevention, cost deferment, labor efficiencies, and risk reduction.

IntelliSee has several examples of customers doing so including:

- Saving a customer more than $150,000 in annual over-time by reducing "just in case" patrolling vs. being directed where to go based on IntelliSee alerts.
- Informing church administrators that a homeless person had taken shelter in their bathroom and that police were on-site with drawn weapons after that person had gone into psychosis.
- Alerting a large school district that teenagers were playing "cops & robbers" with masks and realistic looking toy guns but letting first responders know it was not an emergency situation.
- Informing a community college that their newly replaced roof was failing prior to substantial water damage occurring and early enough the issue could be resolved without involving legal (we also informed a large K-12 district that their newly built second high school had a failing roof).
- Helping a manufacturer receive an insurance discount via assisting their safety and security efforts while helping another discover an employee had become unhoused and was living on property.
- Helping several organizations replace cleaning crews sleeping instead of cleaning, stopping dozens of burglary attempts including thieves cutting fences to access building materials, and more.

IntelliSee's approach provides autonomous detection- / incident-based situational awareness so harm can be minimized and resources can be focused on prevention - e.g., stop a gun before it enters; clean a spill before someone slips; fix a leak before significant damage; stop a trespasser before they break-in or vandalize, etc. If an incident is in process, minimize its severity / impact through these same capabilities.

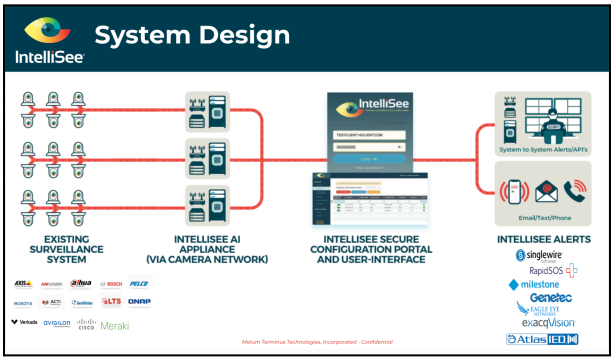
For example, visually detecting drawn guns is an important new safety layer that enables organizations to stop assailants before they can do harm, before shots are fired (vs. sound-based technologies) and - If the event is in process - find assailants quickly in the chaos of the event. Visually detecting drawn guns can be the fastest detection method in both mass casualty events and targeted violence shootings.

- Assailants generally stage or begin shootings in exterior locations - visual detection enables response tactics before the assailant enters targeted buildings.
- Staging areas are often purposefully chosen to be areas without eye witnesses (e.g., stairwells, parking ramps, etc.); However, many are covered by surveillance cameras.
- Eyewitnesses can become incapacitated, panic, or flee before alerting authorities so autonomous visual detection can be more reliable than human eyewitnesses.
- An active shooter event is extremely chaotic - autonomous visual detection can provide the shooter's current location to first responders and those on-site.
- Doing the above via existing cameras avoids adding additional infrastructure or staff ***and*** avoids impacting the learning environment vs. other more conspicuous solutions (e.g. metal detectors).

Similar considerations apply to IntelliSee's other detectable risks. For example, smoke and fire can be visually detected up to 20 minutes before smoke detectors / sensors (plus sensors generally don't work outside). Autonomous monitoring paired with real-time / near real-time alerts improves safety and provides financial savings while leveraging existing infrastructure.

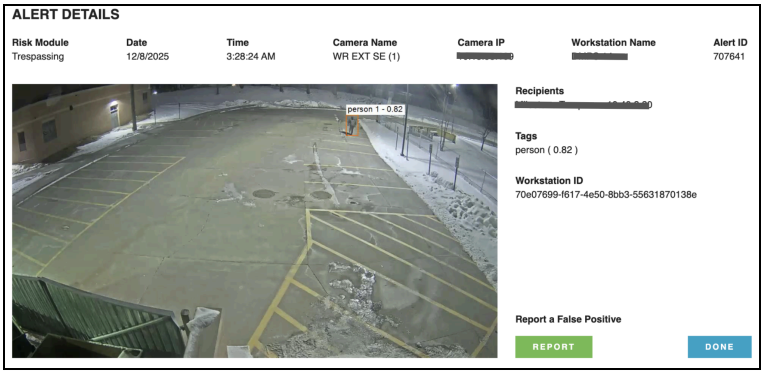
System Description (Functional)

The below illustrates the high-level system flow for IntelliSee (a detailed architecture is provided in the technical section). The application runs on AI servers securely located at customer data centers within their firewall, managed within their protocols. IntelliSee servers connect to the customer's security camera network to analyze camera live feeds. This is generally directly to the cameras via their real-time streaming protocol (RTSP feeds) but connection methods may vary depending upon the customers' infrastructure (e.g., analogue cameras require encoding, some cloud cameras require accessing streams via bridges or the VMS, sub- / de-warped streams are processed on fisheye cameras, etc).



IntelliSee compliantly and ethically balances safety with privacy and other considerations. IntelliSee does not use, store, nor transmit personally identifiable information (PII) nor do we perform facial recognition, license plate recognition (LPR), or any other PII or biometric analytics. Rather, IntelliSee's AI monitors surveillance cameras' live feeds based on the real-time analysis of pixel combinations and patterns.

Camera streams are monitored but not stored nor transmitted. Rather, they are ignored if nothing is detected. If something is detected, a series of real-time / sub-second activities ensue within IntelliSee's application to validate initial detections. This includes concurrent AI networks and sub-second application logic. Confirmed detections are then promoted to alerts (see example on right). Once promoted, alerts are sent to customer designated recipients (including other systems) by risk / threat type and other criteria. Alerts contain the reason for the alert, camera name/location, timestamps, and visual evidence. Alerts do not contain any PII.



Brandished / drawn gun detection includes 24/7/365 human verification and 911-escalation. Monitoring teams receive alerts in real-time and evaluate them within 2-5 seconds to do the following:

- If an active shooter, immediately notify 911 and the customer / release the alert.
- If the rare false positive (see example on right), flag it but don't alert anyone - these assist IntelliSee's AI learning / training.
- If ambiguous (i.e. not an emergency nor an apparent false positive), err on the side of caution. Inform the customer a potential issue may warrant investigation but do not escalate to 911 (these alerts indicate reviewers are releasing it as an ambiguous alert). Customers may then inform 911 through their other existing protocols and procedures.

Other alerts (e.g. spill detection, etc.) are sent without human verification or 911 escalation unless customers choose to do so themselves (e.g. they wish to inform first responders about a potential trespassing after seeing IntelliSee's alert).

All alerts can be sent natively via our text, email or phone services but IntelliSee is purposely designed to integrate as an open system / overlay so customers can send alerts through their other existing systems. These "system to system" alerts are enabled via multiple methods depending upon the receiving system (webhooks, API's, JSON strings, etc.). Examples include:

- Sending alerts through their SMTP/messaging environment(vs. IntelliSee's) where they manage distribution lists and create shared addresses (e.g. intellisee_falls@<customer>.com).
- Sending alerts through communication systems like Singlewire Informacast where other systems (e.g. PA, Access Control, GeoComm, etc.) are integrated and triggered and where communication protocols and lists are managed (see example here).
- Sending alerts to / through video management systems like Milestone, Genetec, and others to trigger other systems, bookmark footage, "pop" video wall screens, and more (see example here).

As a result, first responders / local law enforcement can be alerted in multiple ways depending upon customer preferences and if / how they've coordinated with law enforcement. For example:

- For an active shooter, alert first responders, building principals, administrators, and safety teams via our monitoring team / RapidSOS partnership given 911 integration and 24/7/365 alert verification.
- With coordination and permission, customers can also add local law enforcement and / or emergency centers to any IntelliSee alert by adding them in the user interface (UI).
- Safety teams and administrators may choose to be alerted to potential trespassing (vehicles or people) situations, falls, or other issues and they then alert first responders if needed.
- Customers may alert facilities and building principals when spills or leaks are detected but they generally don't alert others - including first responders - given they are not generally emergencies.

The secure user interface (UI) contains a live alert log that enables additional reporting (described further in the reporting section of this document). Some organizations with security operations centers (SOC's) monitor IntelliSee's live alert log as yet another method of gaining situational awareness.

There are also maintenance-related, administrative alerts including disconnected / non-transmitting camera alerts, system health, system status and other health metrics. These are for system administrators and managed through the user interface (UI). IntelliSee does initial configuration but user administrators are enabled to do so themselves or via IntelliSee. IntelliSee also monitors system health across customers.

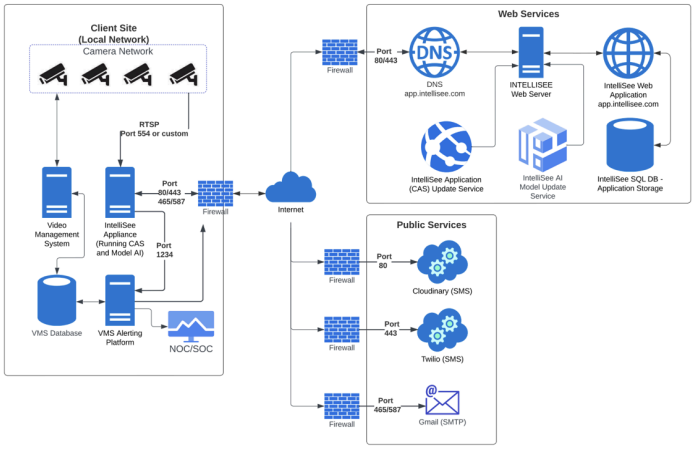
Customers decide what cameras they wish to **M**onitor, what risks to **D**etect and what people and/or systems to **A**lert when something is detected. Settings are configurable - including by camera, time of day, day of week, and by alert recipients (people and other systems) with all settings backed-up remotely should there be a local event affecting the customer's data center and / or should a server suffer a failure. Servers warranties are 3 years with additional detail provided in the support section of this document.

For the purposes of clarity and per the questions listed in the RFP, IntelliSee is designed to leverage a customer's existing surveillance infrastructure. As such, there are no remote devices to mount, to power, or to consider from an all-weather capability. IntelliSee provides AI servers containing the IntelliSee application that reside on-site within customers' climate controlled data centers / data closets.

System Description (Technical)

IntelliSee's service includes its AI application (software); on-site AI devices/servers (hardware); configuration / training activities (labor); and ongoing support, updates, and upgrades (support).

A typical installation's architecture is shown (see image) but this may vary by customer depending upon their camera systems, network architecture, and cybersecurity protocols / requirements.



IntelliSee is U.S.-based with proprietary software developed by its U.S. developers. IntelliSee hardware is supplied by our U.S. supplier (Supermicro) using U.S. components. The user interface is securely hosted in the U.S. by a U.S. hosting provider (Cyberlynk) with all servers located in the U.S. IntelliSee's secure cloud server is located in Milwaukee, WI with redundancy in multiple other U.S. locations should there be a catastrophic event impacting this primary location.

IntelliSee's AI servers are located onsite within customer data centers and within the customer's firewall. Multiple live camera feeds are processed concurrently by these appliances so sizes and capacity vary by the number camera views are being actively monitored. Hardware specifications are listed below.

IntelliSee Hardware Specifications								
Capacity	**OS**	**CPU**	**GPU**	**RAM**	**Storage**	**Size**	**Rack Units**	**Power**
10 views	Windows 11 Pro and / or Server	AMD Ryzen™ 9 7950X	1X NVIDIA Quadro RTX 4000	128GB	2TB NVMe	1.7 x 17.2 x 16.9	1RU	1X 500W
40 views	Windows 11 Pro and / or Server	AMD Ryzen™ 9 9950X3D	2X NVIDIA Ada L4 24GB	128GB	2TB NVMe	3.5 x 17.2 x 25.5	2RU	2X 800W
80 views	Windows 11 Pro and / or Server	AMD Ryzen™ Threadripper™ Pro 9965WX	4X NVIDIA Quadro RTX 4000	256GB	2TB NVMe	3.5 x 17.2 x 31.7	2RU	2X 2000W

Multiple appliances can seamlessly be used together for large customers monitoring more than 80 camera views. Next generation GPU's and larger capacity servers are continually evaluated so specifications are subject to change. To date, we have ensured backward compatibility with any hardware changes.

Once racked, servers are powered and then connected to the surveillance camera network via an ethernet cord plugged into an approved switch on the camera network. A secure internet connection is then opened to configure monitoring, detection, and alerting parameters remotely. Secure port access is also used for updates and if emailing / texting through IntelliSee (vs. leveraging system-to-system alerts integrations). All transmissions are two-way encrypted and follow standard cybersecurity protocols. After configuring, servers are managed by customers within their standard data center and network support protocols.

IntelliSee's Windows-based application runs as a service on IntelliSee's local / on-site servers and consists of the following components:

- **Camera monitoring services** - IntelliSee connects to live camera feeds and analyzes the pixel combinations in real-time. IntelliSee can process any range of resolutions and camera frames per second (FPS); Connection methods depend on the customer's environment but IntelliSee is compatible with nearly every environment and nearly every camera type.
- **Detection services** - This leverages IntelliSee's AI to detect visible risks and threats based on pixel combinations. IntelliSee has multiple proprietary CNN's validating detections in real-time that are further supplemented by downstream, sub-second logic prior to a detection promoting to an alert.
- **Alerting services** - Detections are promoted to alerts upon real-time system verification rules. Gun alerts also have human verification by IntelliSee's dedicated 24/7/365 response team in case they need to be further escalated to 911 / first responders

  Alerts are sent to designated customer personnel and / or to other designated downstream systems (e.g., VMS, MNS, Access Controls, Mapping Software, etc.). Alert integration methods vary (Webhook, API, JSON, etc.) and alerts can also go directly to recipients via SMS, email, or phone calls. 911 escalations are done directly through data transfers and calling if done by IntelliSee.

  Alerts are time-stamped and geo-located; Recipients (including downstream systems) can be tailored by threat types/levels and other criteria (e.g. send leak / spill alerts to Facilities but trespassing to Safety teams). Levels include base, escalated, and severe.
- **User Interface (UI)** - Configurable settings, user administration, alert logs, and other activities are executed via IntelliSee's secure customer portal and web interface. These settings then direct on-site servers. Administrators have credentialed access to the UI.

IntelliSee's proprietary AI was developed by our computer vision engineers who regularly train proprietary convoluted neural networks (CNNs) and do on-going research / testing. As the basis of our AI, IntelliSee has millions of incident video frames from a broad range of sources:

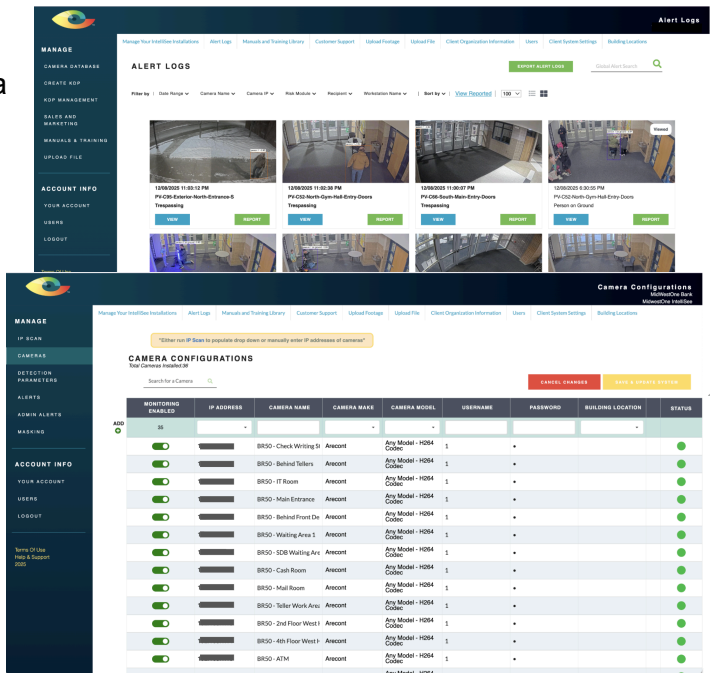
- Data represents a wide variety of risk types (e.g. longguns, handguns, etc.) across a wide variety of camera types, viewing angles, distances, lighting conditions, backgrounds and so on.
- Live footage was initially gathered by contracting with the University of Iowa Campus Police, Iowa City Police, local businesses, and others to enact staged events with real, unloaded guns in front of actual surveillance cameras to represent a broad variety of measured distances, angles, backgrounds, and other situations.
- Data has continuously expanded through a variety of means including but not limited to customer-supplied data, lab tests, live tests, synthetically generated data (e.g., green screen equivalents), publicly available data, and other sources.
- All visual data is from a surveillance, body cam, or vehicle camera point of view. This data is further supplemented via augmentation processes (e.g., rotations, adding blur, color changes, etc.) used by IntelliSee's computer vision engineers to add additional variability to the data.

- Synthetic / green-screen data combines real background data with manipulated risk-type data (e.g. guns, falls, smoke / fire) and vice versa to increase the amount of realistic variance in the data.
- Synthetic data is combined with real data to enhance AI training but validation and test data sets (including videos) do not leverage synthetic data.
- Resulting AI models are run through a litany of performance metrics and lab testing prior to release.

IntelliSee leverages **deep-learning AI**, the most advanced AI that mimics how the human brain learns:

- IntelliSee's AI continually trains with new data and capabilities; Models deploy every ~2 weeks.
- IntelliSee also has a proprietary "active learning" process that further hastens AI learning
- Retrainings also include occasional false positives so IntelliSee's AI can learn from its mistakes
    - False positive rates are very low due to IntelliSee's multi-layered approach; IntelliSee's alert monitoring team further mitigates these and report them to IntelliSee's engineers
    - 911-escalation only occurs if the customer selects that option ***and*** if the situation is an emergency; Ambiguous situations alert the customer but do not escalate to 911
- OTA updates automatically deploy via tailorable processes accommodating customer IT protocols

IntelliSee's intuitive user interface (UI) enable **M**onitoring, **D**etection, and **A**lert parameters and other features such as administrative alerts, masking camera views (e.g. line crossing), sensitivity settings, and so on to be configured. These settings then direct IntelliSee's on-site AI appliances. The secure UI also contains alert logs, documents (e.g. user manuals), and other resources. Customers log-in to the UI via IntelliSee.com with their credentials.



Credentialed roles include admins (those managing the system), users (those who can access the system / alert logs), and alert recipients (those receiving alerts but who do not access the UI). There are no limits to the number of these roles. Administrators access the UI via the standard browsers on desktops and / or mobile devices.

Alert recipients receive alerts in a variety of means including via the customer's other internal systems if desired. Alert settings - including desired mediums - are set by admins and / or IntelliSee (on their behalf) within the UI.

Alerts are stored on local appliances and logged in the UI. Alert logs store alert meta data and retrieve imagery from local devices. Alert images are swept from local appliances after 30 days but alert meta data is stored indefinitely. Historical reporting, exporting, analysis, and other user activities are enabled on the alert logs. This is explained further in the reporting section of this proposal. Any data stored on the UI is fully segregated by customer and each customer's data is protected from access by any other customers (and vice versa).

On-going use and maintenance generally consists of receiving alerts, changing any parameters, adding / editing alert recipients, and / or leveraging any new capabilities released by IntelliSee. OTA push updates are automated by default but can be tailored to customer's protocols. Updates include AI enhancements / learning, new capabilities, and patches. These generally occur at 1am Central on Saturdays but can be pushed at any time by IntelliSee. Releases go through test/development/production processes and also include field testing (we have test units located in our facilities and at some customers).

Customers receive monthly newsletters, release notes, and regularly scheduled meetings to ensure customer satisfaction. On-going use also includes the following:

- Admins can choose to receive automated daily heartbeat / status as to the health status of their installation, camera connectivity status, and other metrics. IntelliSee also monitors system health.
- Support specific alerts are also enabled to inform admins if temperature standards are being exceeded, if camera connectivity is disrupted, and other support related issues.
- Annual or more frequent testing is enabled during normal business hours (or any other time) via multiple methods including temporarily setting up alerts to trace them throughout the process: e.g.;
    - Temporarily set "No person present" alerts on cameras where no person is present
    - Temporarily set "Person detected" alerts on cameras with people in view
    - Etc.
- IntelliSee continually develops enhancements based on customer feedback / requests; We are seeking Iowa Department of Management perspectives for additional enhancements.

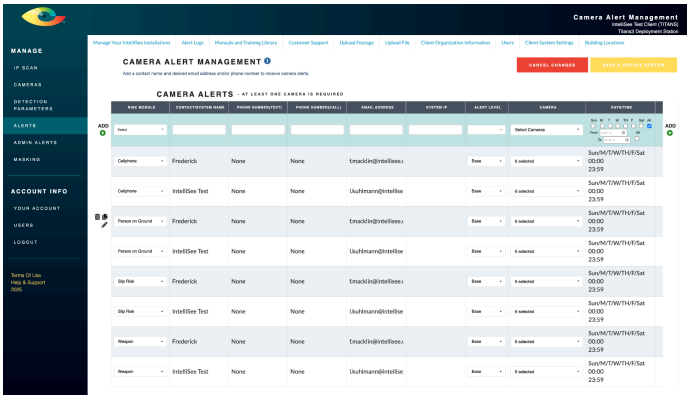
System uptime is 24/7/365 and server warranties are 3 years should a failure occur. IntelliSee has on-hand servers and our supplier (Supermicro) has quick ship capabilities and 24/7 customer support. Customer configurations are backed remotely and can be reset within 2-3 minutes of server reinstallation.

As an emerging Iowa technology firm, we are mid-flight in securing third-party designations but certifications are on roadmap and we are making steady progress as we grow. Specifics include:

- Multiple processes and procedures are documented and maintained as we build out and progress toward additional 3rd party certification (see example here).
- IntelliSee employs monitoring services via New Relic and we perform regular penetration testing in addition to the security, monitoring services, and multi-location redundancy provided by our web host (Cyberlynk).
- Endpoint Detection & Response (EDR) is monitored by our monitoring service's and web host's security operations center 24/7/365.
- The company is actively working toward Federal Risk and Authorization Management Program (FedRAMP) compliance; Similarly, we are not yet ISO/IEC27001 and SOC 2 Type II certified although we adhere to the principles of those standards.
- We are a Department of Homeland Security Safety Act Qualified Anti-Terrorism Technology (QATT); This process requires similar processes and procedures as the above certifications.
- We have also received numerous awards from third parties related to our innovative technology and safety breakthrough (see examples here) and have several customer references.

System Administration

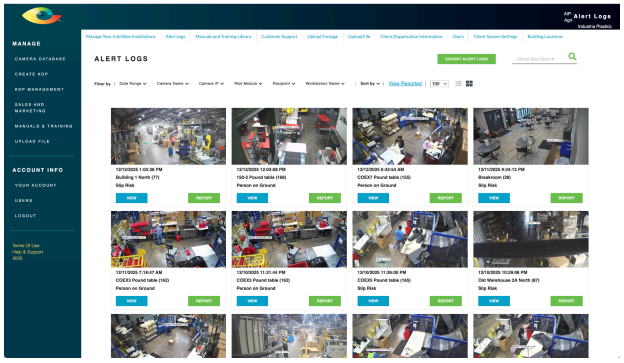
System administrators have access to the IntelliSee portal / UI to direct the on-site, secure AI appliances, to set-up users / alert recipients, and set other configurable settings on the system. IntelliSee and / or IntelliSee reseller partners can do these activities as well if the administrator chooses. Alert recipients do not have system access unless administrators also give them credentials.



Administrator activities can include:

- Adding users / alert recipients
- Add/edit/delete camera views to monitor - including toggling on/off different views
- Add/edit/delete detection parameters - e.g. add detections, set days / hours, etc.
- Mask camera views - e.g. line crossing
- Add/edit/delete alerting parameters - e.g. new employees or PTO, the customer added a new comms system, etc.
- Add/edit/delete admin alerts - e.g. disconnected cameras, daily heartbeats
- View alert logs, filter / analyze alert logs, export alert log meta data, etc.
- Access electronic user manuals and release notes

Reporting



Reporting is primarily related to historical alerts via the IntelliSee alert log. This is a “live” log so it updates in real time as alerts occur. As such, some IntelliSee customers have staff monitor it as an additional alert medium. Administrators and users have credentialed access to logs but alert recipients do not (unless they are both an admin and an alert recipient).

Alert Log reports include the alert meta data and alert images from the local AI appliances. Meta data is stored indefinitely but images are swept from appliances after 30 days. Many customers will bookmark footage in their Video Management System (VMS) based on IntelliSee alerts for incidents. VMS bookmarking then retains that footage by preventing it from being swept in the VMS’ standard cycle but that is outside of the IntelliSee application.

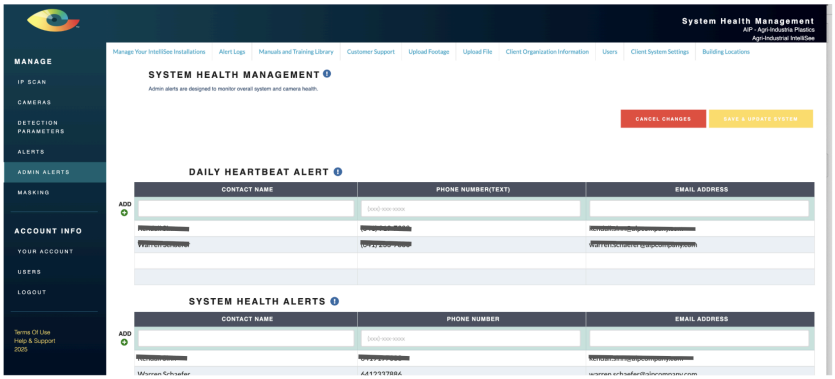
Alert Logs can be presented in multiple views, filtered, sorted or analyzed in multiple ways. For example:

- Date ranges
- Locations / cameras
- Type of incident / risk
- Recipients
- Etc.

This facilitates historical tracking, understanding incident “hot spots”/times/locations, and other reporting. This data can also be exported to facilitate additional analysis, combination with the customers internal data, management reporting, and other activities.

Customers have not requested additional reporting functionality but - as with all development efforts - should they indicate a need or that additional functionality should be a priority, enhancements are added to our development queue.

System health / status reports are primarily managed through the Administrative Alerts / Reports that include system health / uptime, camera connectivity status, appliance temperatures, and other key information.



Customer Support

Another core component of our mission is IntelliSee is our focus on customer satisfaction through a customer-centric culture. IntelliSee’s reseller partners share this same perspective. IntelliSee’s service includes on-going user and technical support; troubleshooting assistance; regular training and documentation; and on-going updates, patches, and enhancements. As mentioned, updates occur every ~2 weeks within customers’ IT protocols and upgrades and enhancements are provided at no additional cost (including the addition of new risk detection capabilities - e.g., smoke/fire, etc.) as we develop them.

IntelliSee assigns a Customer Success contact for each account for these activities (IntelliSee’s Customer Success also works with IntelliSee’s resellers to ensure customers are supported and satisfied). IntelliSee’s Customer Success team has internal technical support through Systems Engineers. System Engineers liaise with other technical staff at IntelliSee, with IntelliSee’s hardware support team, and others - including IntelliSee reseller technical staff and customer technical staff.

IntelliSee has a standardized installation and on-boarding process that is tailorable by customer. Support initiates within this process and it is further described in the next section (section 2.6.7). On-going support extends beyond the initial installation period and continues throughout the customer’s subscription. This includes regular standing meetings with customers, ad-hoc training and update sessions (as customers on-board new employees and / or as IntelliSee releases new capabilities, and so on).

Standard support requests and non-critical incidents are responded to within 24-hours and generally involve Tier 1 support. Tier 1 support is accomplished via IntelliSee Customer Success roles and / or IntelliSee resellers. Tier 2 support includes incidents - both critical and non-critical - that go beyond semi-technical resources and, should they occur, involve IntelliSee System Engineers and other IntelliSee technical staff with IntelliSee Customer Success keeping all parties informed. Reseller technical staff may be involved in these as well. Tier 3 support extends to include IntelliSee’s computer vision engineers, application developers, hardware supplier, our web host service provider, and others as needed.

Standard IntelliSee support hours are weekdays from 8am to 5pm U.S. Central Time. However, IntelliSee staff and our support infrastructure are available at all times regardless of time or day should a critical incident occur (representatives are available across time zones). IntelliSee reseller partners also have dedicated support staff and incident handling. In many cases, IntelliSee's reseller partners already have existing relationships with IntelliSee's customers for other products and services. Customers may initiate support directly with IntelliSee and / or with IntelliSee's reseller partners. IntelliSee and our reseller partners ensure coordination amongst each other and with the customer and their designated staff.

Given IntelliSee's health monitoring, critical incidents (e.g. hardware failure) should be anticipated vs. reactive. Acknowledgement of a critical incident will be proactively reported by IntelliSee staff to customers based on our system monitoring. Customers are also encouraged to apply their existing system monitoring tools to the IntelliSee servers given IntelliSee is part of their broader system infrastructure. Resolution timing will be situational but continual communication will occur throughout the process until resolution.

Alert monitoring staff review alerts 24/7/365. Alert monitoring and 911 escalation has built-in redundancy across geographic locations via our partnership with RapidSOS. IntelliSee's dedicated team consists of multiple staff members regularly trained on IntelliSee alerts and escalation criteria.

Monitoring staff attend bi-weekly meetings to review service levels, update any operational procedures, clarify any edge-cases or ambiguous situations, discuss and answer any additional questions, and to ensure on-going training for existing and new staff.

Through our partnership with RapidSOS, 24/7/365 alert verification and 911 escalation is done by rigorously trained staff specifically dedicated to IntelliSee. Training includes:

- **Introductory Training:** This includes at least 120 introductory hours to prepare them for the role.
- **"Gradation":** After initial training, agents enter an ongoing training program called "Gradation" that takes up to 1.5 years to ensure continuous learning and expertise development.
- **TMA 5-Diamond Certification:** This is a recognized industry standard for monitoring centers and it specifies a high level of expertise is awarded upon Gradation completion.
- **Standard Operating Procedures (SOPs):** Training covers specific protocols for various types of IntelliSee alert situations.
- **Technology and Data Handling:** Agents are trained to receive and interpret IntelliSee alerts, when to escalate, and how to efficiently transmit this data to 911 dispatchers (local PSAPs) if escalated.

IntelliSee's dedicated team is explicitly trained on specific alert situations and criteria related to brandished guns and smoke / fire.

Regarding active shooters:

- If an active shooter situation has been identified and the customer has chosen to enable 911 escalation by IntelliSee: notify first responders, release the alert, and notify the customer.
- If the situation is false positive, do not release the alert but flag it as such (at which point it is automatically added to IntelliSee's data process to assist our AI's learning)

- If a situation is ambiguous (i.e. not an apparent active shooter nor an apparent false positive but may be of concern), err on the side of caution and release the alert to the customer but do not escalate the alert to 911. These alerts indicate Potential Weapon Detected - Unclear.

Given the lower urgency and real-world situations of other detected risks / threats (e.g. spills, leaks, potential trespassing, etc.), those alerts do not include 911-escalation. If the customer chooses to alert first responders on these, there are multiple methods of doing so:

- Based on the real-time situational awareness IntelliSee enables, customers may alert first responders directly or through their downstream systems (e.g. their mass notification systems) should they believe the situation warrants that (e.g. IntelliSee detected someone cutting through a fence or a suspicious vehicle in an unauthorized area).
- Many schools have local agreements with their local law enforcement and / or emergency services. If the customer has coordinated with them, they can be added as alert recipients to the customer's IntelliSee installation (e.g. alert facilities, building administrators, and the local police if a vehicle or person is identified in a specific area between the hours of midnight to 4am, etc.).

2.6.7. Implementation Plan

With upfront prep, implementation is quick and easy. Most steps are done remotely per the customer's requested schedule and all can be completed within the customer's IT protocols. Steps consist of gathering information most organizations have at their ready and this document contains a checklist of these pre-installation activities. IntelliSee and / or its reseller partners perform these with customers:

- Confirming camera views, counts, and networking approaches
- Pre-gathering camera credentials and IT security protocols / port access
- Determining administrators, users, and alert recipients (including other systems)
- Ensuring the physical environment for the IntelliSee AI appliances meets specifications

IntelliSee consults and advises throughout these steps - including advising on camera views. IntelliSee's detection guidelines (link) are based on testing and surveillance data realities that include:

- If the human eye or camera can't see something, neither can IntelliSee
- Distances, lighting, and angles matter (ie., the physics of optics matter)
- Artificial intelligence is not the same as human intelligence (not yet at least) so some detections may be accurate but are not incidents (e.g., a child laying on the ground vs. a person who fell)

The customer's time investment is generally unburdensome given most organizations have the needed information readily available. Historical estimates range from 30-60 minutes to gather this information and / or to meet with IntelliSee to review these together. Typical school functions include administration (sponsor), IT, Safety Teams, HR and Facilities. Of these, point functions vary but it is fairly typical for smaller schools to manage these activities through their IT staff whereas larger schools often manage them through their Safety or Facilities teams (whomever is managing their surveillance cameras).

IntelliSee and our reseller partners shepherd customers through the process. Once specifications and customer needs are understood, IntelliSee secures hardware, installs and tests the IntelliSee software, and drop-ships to the customer's desired location (hardware and environment specifications are listed here).

Most customer IT teams prefer to rack IntelliSee servers themselves. IntelliSee and / or our partners can also physically install upon customer request / permission and data center access. Once racked, servers are connected to the customer's camera network and a secure port is opened for internet access. Through this access, IntelliSee remotely configures the application to customer specifications. IntelliSee's default access is via TeamViewer but, like other settings and security protocols, IntelliSee conforms to customer IT protocols so we are experienced configuring each installation via multiple methods.

IntelliSee has implementations ranging from 10 camera views to installations exceeding thousands of views. IntelliSee conforms to each organization's IT, cybersecurity, or other requirements so nearly every implementation is slightly customized. Similarly, IntelliSee pushes regular OTA updates within each customer's protocols. Updates are automated by default but these are also adapted per customer needs.

The schedule on the next page is typical for installations across all sizes of organizations. End-to-end processes take ~4 weeks but can vary depending upon customer schedules, availability, and desires. Server fulfillment takes 1-2 weeks during which time pre-installation / -configuration tasks are completed.

Installation and configuration typically occur on the same day at which point alerts are initially sent to IntelliSee as our AI learns the environment and to fine tune sensitivities and other settings. System admin and alert recipient training is scheduled during this time as well.

Go-live is set by the customer and is defined when recipients begin receiving alerts. Typical timelines from order to go-live is approximately 4 weeks but can extend if the customer wishes for a different schedule.

Once the customer has gone live, weekly sessions are scheduled for questions, feedback, and any changes (admins are also enabled to make changes). After 2-4 weeks and per customer desire, session frequency generally reduces to regularly scheduled check-ins (monthly or quarterly depending upon the customer). Ad-hoc sessions also occur at no additional cost as customers add or change staff, as IntelliSee releases new capabilities, to expand coverage, and so on.

Typical Project Schedule
Below are the items and schedule to implement the IntellISee solution:

No.	Item	Resources	Due Date
1	Review Surveillance Camera Views: • Evaluate and review existing camera views • Gather camera IP addresses, names, makes / models, physical addresses/geo locations, usernames, and passwords. • Determine risks/threats to detect by view and by daypart • Begin defining alert recipients by medium and dayparts	Customer & IntelliSee	Effective Date
2	Preparation & Appliance Installation. • Camera network(s) configuration confirmed • Physical locations and rack space for appliances confirmed • Data center(s) power, switch capacity, and cooling confirmed • Installation scheduled with/ monitor, keyboard, and mouse available	Customer & IntelliSee	Effective Date +10 Days
3	Programming & Configuration. • IntelliSee portal set-up • Camera and alert information added • Program monitoring, detection, and alert parameters • Determine any masking or sensitivity adjustments	IntelliSee w/ Customer	Effective Date +10
4	System Validation & Testing • Add IntelliSee as alert recipient (during AI burn-in period) • Evaluate initial detections and alerts • Configuration adjustments (parameters, etc.) • Add customer alert recipients	IntelliSee & Customer	Effective Date +24
5	Training & full implementation • General overview & process • Initial alert review • System administrator training • End-user training	IntelliSee w/Customer	Effective Date +31

Documentation and training (including future / ad-hoc training) is provided at no additional cost throughout this process. Documents include the following and other materials as needed / desired:

- Pre-installation checklist (link)
- Installation quick-start guide (link)
- Installation guide (link)
- IntelliSee user-manual (link)
- Admin training presentation (customized for each customer)
- User and alert recipient training presentation (customized for each customer)
- Release notes and monthly newsletter

Customer engagement ensures a successful and timely go-live. Customer responsibilities include:

- Determine points of contact / administrators for the IntelliSee platform
- Gather and provide specifics about their surveillance camera systems:
    - Camera makes / models, IP & physical addresses, credentials & naming conventions.
    - Camera views to monitor (given IntelliSee's customer-friendly license, it is recommended that all cameras be loaded…monitoring can be switched amongst cameras as needed)
    - Threats / risks to detect where and when (i.e., detection parameters); IntelliSee assists this process with additional capabilities (e.g., sensitivity sliders, masking, etc.)

      Please note: Given IntelliSee's customer-friendly license, none of the above are permanent decisions. Customers can monitor different cameras, change detection parameters, and/or change alerting parameters/recipients at any time.
- Coordinate and align with the customer's IT staff:
    - IntelliSee works with IT teams to secure network specifics and to ensure IntelliSee adheres to their network and cybersecurity protocols.
    - IT also ensures data center access, appliance installation, network connections, and secured ports are opened within the customer's network(s).

      Please note: IntelliSee proposals do not include labor to support any site-specific IT security requirements, such as loading additional software, specific Windows versions, etc. but these are options.
- Identify locations for the IntelliSee appliance(s) and ensure physical environments are prepared:
    - Provide locations for the data centers/closets where IntelliSee appliances will be located
    - Ensure there is sufficient rack space and power, switch capacity, and cooling are sufficient.
    - This document outlines physical and other requirements for the IntelliSee platform.

      Please note: IntelliSee's data center requirements are consistent with the vast majority of organizations' existing environments. Any data center or network enhancements required to operate the IntelliSee system are performed by IntelliSee resellers and / or are outside of the scope of IntelliSee's proposal.
- Identify and prepare the customer's internal teams and any external partners (e.g. first responders):
    - Align with Risk, HR, Finance, or any other teams dealing with staff safety, insurance, or other costs associated with any incidents.
    - Consider who should be informed that the organization is investing in additional safety (e.g., many organizations highlight these investments to staff and other key stakeholders)

Training

Training is a key component of the IntelliSee process from two perspectives:

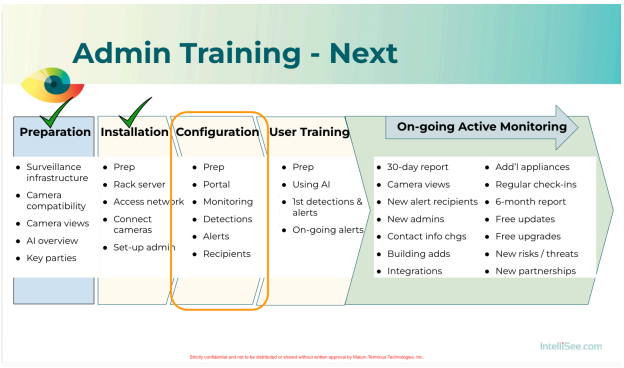
- There is a "burn-in" period of time where IntelliSee's AI trains on the customer's environment
- From a customer perspective, administrator and alert recipient training occurs throughout

AI training involves adding customer camera views, any historical footage, or any other visual data the customer has that would benefit IntelliSee's neural networks' learning. This data assists IntelliSee's computer vision engineers and we refer to this as the AI burn-in period. This is part of the installation process and IntelliSee has automated processes (with the exception of any customer supplied incident

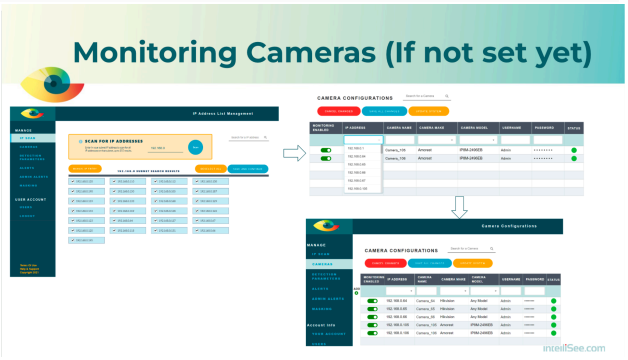
footage) to fulfill these steps. During this period, initial customer training is also occurring and alerts are sent to and reviewed by IntelliSee to make any necessary configuration adjustments.

Customer training initiates within the implementation plan / project schedule starting with administrator training on how to use and leverage the IntelliSee application. These are scheduled as installation specifics finalize and sessions are typically 60 minutes and are done as virtual live sessions.

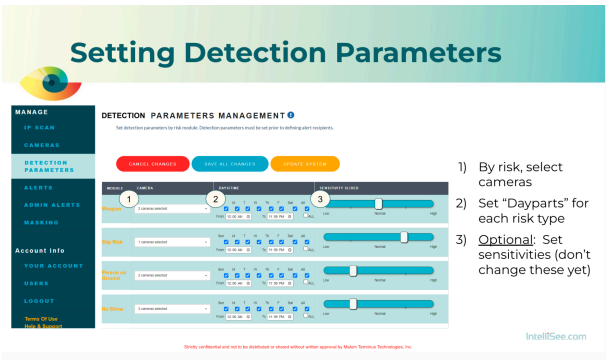
Training involves presentations and hands-on activities that are also included in IntelliSee's administrator's manual. Attendees are also shown the manual and how to access it in their UI / portal. Sessions can be broken into separate sessions, repeated with administrators, or include others if the customer desires so (all at no additional cost).



Content includes re-grounding on IntelliSee and its detections / alerts, a brief overview of AI (including its limitations), a review of the IntelliSee application, and hands-on training on the user-interface (UI). Administrators point and click through steps with guidance after being shown by IntelliSee (this assists in knowledge retention).



Although IntelliSee does initial system configurations, this hands-on training includes how to: **M**onitor cameras; set **D**etection parameters; how to set up **A**lerts and alert recipients; how to set-up administrative alerts; setting up users; setting other features (e.g. camera view masking, etc.). Administer training is typically 45-60+ minutes depending upon customer wants and number of participants.

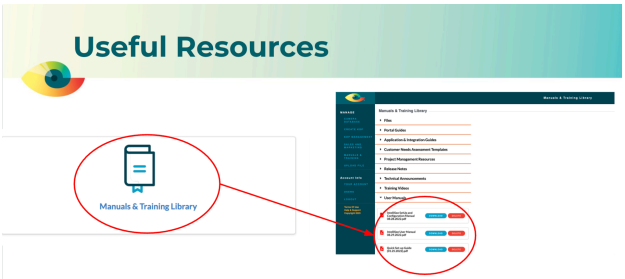


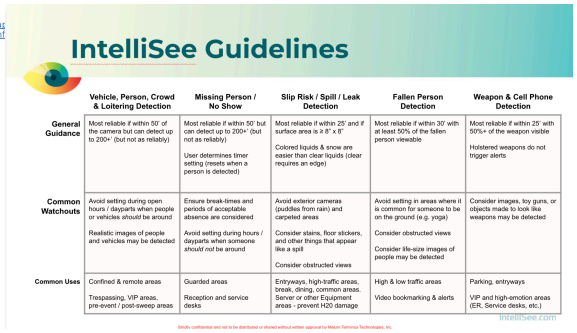
Alert recipient training is also scheduled during the AI "burn in" period. This training is coordinated with system administrators (and / or project sponsors) after administrator training. Sessions are typically 30-45 minutes depending upon customer wants and number of participants. Content includes a brief overview on IntelliSee and AI but then detail on IntelliSee alerts and the alerting process.

Alert recipient training does not include UI training and other components included within the administrator training but attendees are informed on who their administrators are (they generally attend as well) and how to get ahold of IntelliSee as well (with the recommendation that they go through their designated administrators / IntelliSee point contacts).

Documentation includes the following and others materials:

- Pre-installation checklist (link)
- Installation quick-start guide (link)
- Installation guide (link)
- IntelliSee user-manual (link)
- Admin training presentation (customized for each customer so are emailed)
- User and alert recipient training presentation (customized for each customer so emailed)
- Release notes and monthly newsletter





Additional and ad-hoc training sessions occur as needed and per the customer's need or desire. This includes refresher training; training any new employees, administrators, alert recipients, etc.; and training on any new IntelliSee features released. Training is generally performed as virtual meetings but can be in person if desired. There is no additional cost for training.

Performance-Based Criteria

Beyond typical financial incentives (e.g. payment terms et al) the nature of IntelliSee's service is not naturally conducive to performance based incentives or disincentives given a customer's risk exposure / profile is highly variable. IntelliSee is open to performance-based criteria with potential considerations for:

- Guaranteeing installation dates within a set period from date of order (e.g. 30-days) and upon completion of the customer's pre-installation checklist and scheduling.
- Shared incentives based on achieved cost reductions or insurance discounts customers achieve.
- Satisfaction incentives or disincentives for an initial period of time or uptime / downtime (e.g. 99%+) incentives or disincentives.
- Others that the Iowa DOM considers or recommends.

For the same reasons, IntelliSee's monitoring personnel are not directly financially incentivized or disincentivized by performance metrics but these play a key role in their performance evaluation and in the bi-weekly review meetings. Metrics include:

- Average time to resolution defined as the number of seconds from alert reception to alert evaluation and response (typically 2-10 seconds).
- Adherence to workflow and escalation protocols and evaluation of their response to edge-case scenarios (e.g. alerts that are neither obvious emergencies nor obvious occasional false positives).
- Stopwatch testing (not literal stopwatches but system speed) on time from customer system alert to monitoring system receipt; These occur in milliseconds.

Results are reviewed bi-weekly but not typically shared beyond IntelliSee's management team.

Section 4: Experience

IntelliSee has been in business since 2020 (5 years) after forming in 2019. We formed specifically to provide the types of goods and services sought by this solicitation. We do so via our singular focus on analyzing a customer's existing surveillance cameras with our deep-learning computer vision artificial intelligence (AI) in real-time to autonomously detect visible risks and threats.

IntelliSee was founded by University of Iowa executives, local business leaders, and technologists from Iowa to help stop the scourge of school shootings. We do so by autonomously detecting drawn / brandished guns - handguns, longguns, assault rifles, and so on. Alpha product was created in 2020, live beta's occurred in 2021, and the company began commercializing IntelliSee in late 2021.

Because IntelliSee is an Iowa-based company founded and managed by Iowans, we have several insurance companies who are investors and / or partnering and advising with us. They indicated that an active shooter incident is *extremely* rare (a very low probability but high impact / high severity risk) and they requested we build a platform that could also help with other risks / threats that cause harm and drive significant cost to schools and others. We took this to heart and developed an expandable platform detecting drawn / brandished weapons (handguns, longguns, assault rifles, etc.) ***and*** other visible risks that affect all organizations (e.g. trespassers, loitering, vehicles, leaks, spills, falls, etc.).

We continually expand this platform - cellphone detection was added this fall, smoke/fire detection is in beta release to current customers, and we are researching and developing additional capabilities for release in 2026. These, like all other enhancements, are provided to customers at no additional cost.

Our sole product is IntelliSee which is designed to meet the needs and requirements outlined in this Request for Proposal (RFP). IntelliSee autonomously monitors a customer's existing security cameras with deep-learning computer vision AI to detect a broad and growing range of visible risks and threats in real time. Alerts provide the situational awareness needed to prevent and mitigate harm. These capabilities have been detailed in prior sections and additional information can be made available upon request.

IntelliSee is focusing on the United States prior to expanding to other countries (despite several inquiries). Installations are occurring throughout the country and we have a large and growing network of partners ranging from other technology firms, insurance companies, resellers / system integrators, and more.

Over time, we have significantly expanded our network of partners including strategic investors, distributors / reseller partners, technology partners, and additional insurance companies including large property & casualty carriers.

Per the requirements of this RFP, below is a list of customer references across a range of sectors and locations. We have more heavily weighted this list to education and Iowa-based customers with a smattering of others. Although we have customers throughout the U.S., we skew more heavily to the midwest given our Iowa-based roots.

Example IntelliSee References				
Client Name	**Sector**	**Location**	**Contact Person**	**Telephone Number**
Waukee Community School District	Education	Iowa	Shaun Flood	(515) 987-5161
Des Moines Public Schools	Education	Iowa	James (Jamie) Wilkerson	(515) 242-7621
Dubuque Community Schools	Education	Iowa	Coby Culbertson	(563) 552-3000
Starts Right Here	Education	Iowa	Will Keeps	(515) 410-1184
Des Moines Christian	Education	Iowa	Jason Gibson	(515) 252-2480
PSD150 Peoria School District	Education	Illiniois	Michelle Seipel	(309) 672-6512
Grand Ledge Public Schools	Education	Michigan	Chris Chester	(517) 925-5775
Concordia University	Education	Wisconsin	Sean Young	(262) 243-4239
Agri Industrial Plastics	Manufacturing	Iowa	Amy Jones	(641) 472-4188
Walsh Door	Manufacturing	Iowa	Marty Walsh	(515) 262-9822
MidwestOne Bank	Financial Services	Iowa	Matthew Fettkether	(319) 356-5800
Oaknoll Retirement	Senior Living	Iowa	Aaron Comstock	(319) 351-1720
Parkview Church	Houses of Worship	Iowa	Jesse Whitlow	(319) 354-5580
Boone County Hospital	Healthcare	Iowa	Evan Jorgensen	(515) 432-3140

It was also requested to share at least three incidents where the proposed system successfully detected a firearm leading to a measurable action. Fortunately, IntelliSee's customers have yet to experience an active shooter situation but there are several instances where IntelliSee has detected actual weapons:

- Police entered a church with drawn guns after a church member discovered a homeless person in the restroom late at night. IntelliSee's alert informed church administration that an incident was occurring at one of their facilities and late night protocols were further enhanced as a result.
- Two teenagers were playing cops & robbers with masks and realistic toy guns that were detected. Police were dispatched but informed that the situation was not a likely emergency and the students were informed on the dangers their activities.
- An SRO drew their weapon to show it to students and others. IntelliSee's alert informed administration and the SRO was reprimanded and instructed to keep his weapon holstered unless there was an actual emergency.

Several other detections have occurred including guns being detected during funeral services (e.g. twenty one gun salutes), ROTC training on school properties, through customer tests, and other situations.

Beyond customer tests, IntelliSee does substantial and on-going testing throughout its development and model release processes. These processes and others have been reviewed by the Department of Homeland Security and they have certified IntelliSee as a DHS SAFETY Act Qualified Anti-Terrorism Technology (QATT). Qualified technologies can be found at: www.safetyact.gov.

IOWA | Homeland Security and Emergency Management

School Security Infrastructure Software and Technology Approved Organization List

The following organizations have attested that they meet all of the statutory requirements as described in the Iowa Department of Homeland Security and Emergency Management's School Security Infrastructure Software and Technology Attestation Form:

Organization Name	Contact Phone Number	Contact Email
ZeroEyes, Inc.	757-615-4478	Robcarter@zeroeyes.com
IntelliSee	866-222-6530	s.keplinger@intellisee.com

IntelliSee is also one of only two firms listed on the Iowa Homeland Security and Emergency Management School Security Infrastructure Software and Technology Approved Organization List. That list can be accessed here but it is also shown to the left.

Unlike alternatives on this list and as noted earlier, IntelliSee goes beyond brandished gun detection to also assist schools and others with their broader safety needs. As a result and given the extremely low likelihood of an active shooter incident, IntelliSee is the only provider on this list that can also generate a return on investment (ROI) for organizations.

IntelliSee has already exceeded scalability requirements for active users but key scale considerations for IntelliSee include:

- IntelliSee's hardware supplier (Super Micro) is a long standing U.S. hardware assembler and distributor who has the requisite scale and experience to continue supplying without disruption.
- IntelliSee will continue to grow its Customer Success and Technical resources commensurately with its customer growth.
- As sales continue to grow, the financial resources to continue developing additional product features will also grow. As an Iowa-based company, this will drive technology jobs within our state.
- From an individual customer perspective, installations can range from as few as 10-cameras being monitored to those monitoring thousands of cameras but we will continue to scale options to facilitate easier and less costly solutions across all customer types.
- Related and as noted in other sections of this proposal, we will continue to progress on securing 3rd party certifications (given the resource commitment required to do so, we have continually prioritized which we will selectively pursue).
- IntelliSee currently works with multiple subcontractors / resellers and has experience doing so but we will continue to scale investments into both supporting customers and partners.

Regarding the last point, IntelliSee ultimately works with schools and others through a variety of means. Our preferred method is to support customers via a combination of IntelliSee resources and our network of resellers / systems integrators. For example, Walsh Door and Security - one of Iowa's longest continuously operating companies - is an Iowa-based partner with teams located throughout the state (and across other states). They have long-standing relationships with many Iowa's schools and others. In many cases, these customers prefer to have Walsh handle implementation activities with IntelliSee given Walsh is familiar with the customer, is familiar with their other systems (e.g. surveillance, VMS, notification systems, access control, etc.), and IntelliSee. Other reseller partners have similar relationships and expertise.

In some cases, IntelliSee does not use subcontractors / resellers given either the customer's requirement. IntelliSee also has a strategic partnership with AtlasIED where IntelliSee can be purchased with their products (public address systems, mass notification systems, etc.) through their distribution network.

Sales through all channels are managed similarly in that IntelliSee and our partners surround and support the customer to ensure a smooth installation / configuration, on-going support, and ultimately safer and satisfied customers.

Section 5: Key Personnel

Key Personnel	Role / Experience
Scott Keplinger Scott has been with IntelliSee since 2020 (5 years) and holds a MS from the University of Wisconsin Madison and a BA from Iowa State	• IntelliSee co-founder, Board member, CEO • Asymmetria co-founder • https://www.linkedin.com/in/scottkeplinger/
Lucas Kuhlmann Lucas has been with IntelliSee since 2021 (4 years) and holds a University of Iowa BBA	• Chief Technology Officer • Former CTO ACT, Security Officer Pearson • https://www.linkedin.com/in/lucaskuhlmann/
Michael Goedken Michael has been with IntelliSee since 2024 after his father (Tom Goedken) retired and has a University of Iowa BBA and University of Nebraska MBA	• Chief Financial Officer (fractional) • Former VP Fin. (MediRevv) and Corp Controller (Tegria) • https://www.linkedin.com/in/michael-goedken-0a710988/
Richard (Dick) Ferguson Dick has been with IntelliSee since 2020 and holds a University of Pittsburg PhD, Western Michigan MA, and Indiana University BA	• Co-founder, Board chair • Chair & CEO emeritus ACT, Ed Tech venture capital • OpenLoop co-founder and board chair • https://www.linkedin.com/in/richard-ferguson-11b48412/
Dan Clay Dan has been with IntelliSee since 2020 and holds a University of Missouri PhD and MBA, and a St. Scholastica BA	• Co-founder, Board member • Dean of the College of Education, University of Iowa • https://www.linkedin.com/in/dan-clay-2b49722a/
Greg Carstensen Greg has been with IntelliSee since 2020 and holds a University of Iowa MBA and St Olaf BA	• Co-founder, Board member • Asymmetria co-founder & president • Ballast Capital founder & president • https://www.linkedin.com/in/greg-carstensen-874567b
John Ivey John joined IntelliSee's board in 2023 and holds a BBA from Arizona State University	• Board member • CEO & Owner AtlasIED / MiTek • https://www.linkedin.com/in/johnathan-ivey-6b33786/
Chuck Wilson Chuck has been involved with IntelliSee since 2020 and joined its board in 2023	• Advisory board member • Founder, CEO emeritus NAHB; Founder PASSK12 • https://www.linkedin.com/in/chuck-wilson-49aa17b/

Beyond senior management and IntelliSee's board of directors, IntelliSee has sales representatives, Customer Success staff, Systems Engineers / Technical Support, Product Management, Application Development, Data Management, and Computer Vision Engineers. Additional details can be provided upon request. The majority of staff reside in Iowa and all resources are either citizens or legally authorized to work in the United States.

As mentioned, IntelliSee has a growing network of partners - including resellers that act as subcontractors in the capacity of this proposal. IntelliSee wishes to submit the following partners / subcontractors for consideration within this proposal. An individual subcontractor within this list may be used for each customer installation, configuration and on-going support. As such, the approximate % of work completed will be roughly the same per project (vs. additive across these subcontractors for each installation).

Company	Address	Contact	Service	Experience	% of Work
Walsh Door & Security	2600 Delaware Ave Des Moines, IA 50317	Nate Hugeback nhugeback@walshdoor.com (712) 790-3270	Installation, configuration, and customer support assistance	IntelliSee's primary reseller and partner in Iowa; Large, established entry systems, safety/security systems, and other system manufacturer, installer, integrator, and servicer who is respected across Iowa K-12's	20%
Basepoint Building Automations	6200 Thornton Ave #140, Des Moines, IA 50321	Abe Wolfe awolfe@basepointba.com (515) 371-0019	Installation, configuration, and customer support assistance	Large, established building systems, safety/security systems, and other system installer, integrator, and servicer who is respected across Iowa K-12's	20%
AtlasIED	4545 East. Baseline Rd Phoenix, AZ 85042	Mark Foerderer mark.foerderer@atlasied.com 913-754-6096	Installation, configuration, and customer support assistance	Large, multi-national technology firm with safety, public address, mass communication, and other related solutions	20%

A subcontractor form for each subcontractor is provided within this document and will be uploaded onto the JAEGGER portal as well.

Section 6: RFP Forms

Attachment #1: Respondent Information Table

IOWA Department of Management

Solicitation No. RFP 185-2528-2026 *Title: Gun & Incident Detection Software*

Attachment #1: Respondent Information

Primary Contact Information (an individual who can address issues re: this Proposal)	
Name:	Scott Keplinger
Address:	808 5th Street, Suite 5, Coralville IA 52241
Tel:	(515)783-6738
Fax:	
E-mail:	s.keplinger@intellisee.com

Respondent Detail	
Business Legal Name ("Respondent"):	Malum Inc.
"Doing Business As" names, assumed names, or other operating names:	IntelliSee
Parent Corporation Name and Address of Headquarters, if any:	Same
Form of Business Entity (i.e., corp., partnership, LLC, etc.):	C-corp
State of Incorporation/Organization:	Delaware / Iowa
Primary Address:	808 5th Street, Suite 5, Coralville, IA 52241
Phone:	(866) 222-6530
Local Address (if any):	2522 NW 162nd St, Clive IA 50325
Addresses of Major Offices and other facilities that may contribute to performance under this RFP/Contract:	808 5th Street, Suite 5, Coralville, IA 52241
Number of Employees:	12
Number of Years in Business:	5 years
Primary Focus of Business:	Artificial intelligence
Federal Tax ID:	83-3868047
UEI #:	N1U1K4H6L1N9 (UEI) 116825743 (DUNS)
If the Respondent is currently registered to do business in Iowa, provide the Date of Registration:	9/23/2019
Do you plan on using subcontractors if awarded this Contract? {If "YES," submit Attachment 2 - Subcontractor Disclosure Form for each proposed subcontractor.}	Yes

Federal tax ID: 83-3868047
UEI #: N1U1K4H6L1N9
DUNS: 116825743

Attachment #2: Subcontractor Disclosure Form

Subcontractor Disclosure Form - Walsh Door & Security

IOWA | Department of Management

Solicitation No. RFP 185-2528-2026 *Title: Gun & Incident Detection Software*

Attachment #2: Subcontractor Disclosure Form

*(Submit this completed form with your proposal submission. Fully complete a form for **each** proposed subcontractor. If a section does not apply, label it "not applicable." If the Respondent does not intend to use subcontractor(s), this form does not need to be returned.)*

Primary Respondent ("Primary Respondent"):	
Subcontractor Contact Information (individual who can address issues re: this RFP)	
Name:	**Nate Hugeback**
Address:	**2600 Delaware Ave, Des Moines, IA 50317**
Tel:	**515-262-9822**
Fax:	**515-262-8315**
E-mail:	**nhugeback@walshdoor.com**

Subcontractor Detail	
Subcontractor Legal Name ("Subcontractor"):	Walsh Door & Hardware Co
"Doing Business As" names, assumed names, or other operating names:	Walsh Door & Security
Form of Business Entity (i.e., corp., partnership, LLC, etc.)	Corp
State of Incorporation/Organization:	Iowa
Primary Address:	2600 Delaware Ave
Tel:	515-262-9822
Fax:	515-262-8315
Local Address (if any):	
Addresses of Major Offices and other facilities that may contribute to performance under this RFP/Contract:	
Number of Employees:	200
Number of Years in Business:	159
Primary Focus of Business:	Commercial Doors Frames Hardware and Security
Federal Tax ID:	42-1113350
Subcontractor's Accounting Firm:	UHY
If the Subcontractor is currently registered to do business in Iowa, provide the Date of Registration:	1/1/1979
Percentage of Total Work to be performed by this Subcontractor pursuant to this RFP/Contract.	
General Scope of Work to be performed by this Subcontractor	
Detail the Subcontractor's qualifications for performing this scope of work	

Page 1 of 2

By signing below, Subcontractor agrees to the following:

1. Subcontractor has reviewed the RFP, and Subcontractor agrees to perform the work indicated in this submitted Proposal if the Primary Respondent is selected as the winning Respondent in this procurement;

2. Subcontractor recognizes and agrees that if the Primary Respondent enters into a contract with the Agency as a result of this RFP, all restrictions, obligations, and responsibilities of the contractor under the contract shall also apply to the subcontractor;

3. Subcontractor agrees that it will register to do business in Iowa before performing any services pursuant to this contract, if required to do so by Iowa law; and,

4. Subcontractor certifies that it will comply with Davis-Bacon requirements if applicable to the resulting contract.

The person signing this Subcontractor Disclosure Form certifies that he/she is the person in the Subcontractor's organization responsible for or authorized to make decisions.

I hereby certify that the contents of the Subcontractor Disclosure Form are true and accurate and that the Subcontractor has not made any knowingly false statements in the Form.

Signature for Subcontractor:	
Printed Name/Title:	Nate Hugeback, Director of Security + Facilities
Date:	12/15/2025

Subcontractor Disclosure Form - Basepoint Building Automations

IOWA | Department of Management

Solicitation No. RFP 185-2528-2026 *Title: Gun & Incident Detection*

Attachment #2: Subcontractor Disclosure Form

*(Submit this completed form with your proposal submission. Fully complete a form for **each** proposed subcontractor. If a section does not apply, label it "not applicable." If the Respondent does not intend to use subcontractor(s), this form does not need to be returned.)*

Primary Respondent ("Primary Respondent"):	Basepoint Building Automations
Subcontractor Contact Information (individual who can address issues re: this RFP)	
Name:	Abe Wolfe
Address:	6200 Thornton Ave, Des Moines, IA 50321
Tel:	515-371-0019
Fax:	N/A
E-mail:	awolfe@basepointba.com

Subcontractor Detail	
Subcontractor Legal Name ("Subcontractor"):	Control Installations of Iowa
"Doing Business As" names, assumed names, or other operating names:	Basepoint Building Automations
Form of Business Entity (i.e., corp., partnership, LLC, etc.)	S-Corp
State of Incorporation/Organization:	Iowa
Primary Address:	6200 Thornton Ave, Des Moines, IA 50321
Tel:	(800) 779-2760
Fax:	N/A
Local Address (if any):	
Addresses of Major Offices and other facilities that may contribute to performance under this RFP/Contract:	6200 Thornton Ave, Des Moines, IA 50321 905 Metzger Dr, Hiawatha, IA 52233
Number of Employees:	200
Number of Years in Business:	42
Primary Focus of Business:	Security, HVAC, Automatic Doors
Federal Tax ID:	42-1201473

Subcontractor's Accounting Firm:	Basepoint Building Automations
If the Subcontractor is currently registered to do business in Iowa, provide the Date of Registration:	1983
Percentage of Total Work to be performed by this Subcontractor pursuant to this RFP/Contract.	100%
General Scope of Work to be performed by this Subcontractor	
Intellisee implementation. Provide software, appliances, licensing, and programming.	
Detail the Subcontractor's qualifications for performing this scope of work	
Intellisee partner- trained techs and programmers for software.	

By signing below, Subcontractor agrees to the following:

1. Subcontractor has reviewed the RFP, and Subcontractor agrees to perform the work indicated in this submitted Proposal if the Primary Respondent is selected as the winning Respondent in this procurement;

2. Subcontractor recognizes and agrees that if the Primary Respondent enters into a contract with the Agency as a result of this RFP, all restrictions, obligations, and responsibilities of the contractor under the contract shall also apply to the subcontractor;

3. Subcontractor agrees that it will register to do business in Iowa before performing any services pursuant to this contract, if required to do so by Iowa law; and,

4. Subcontractor certifies that it will comply with Davis-Bacon requirements if applicable to the resulting contract.

The person signing this Subcontractor Disclosure Form certifies that he/she is the person in the Subcontractor's organization responsible for or authorized to make decisions.

I hereby certify that the contents of the Subcontractor Disclosure Form are true and accurate and that the Subcontractor has not made any knowingly false statements in the Form.

Signature for Subcontractor:	Abram Wolfe
Printed Name/Title:	Abram Wolfe
Date:	12/16/25

Subcontractor Disclosure Form - AtlasIED

IOWA Department of Management

Solicitation No. RFP 185-2528-2026 *Title: Gun & Incident Detection Software*

Attachment #2: Subcontractor Disclosure Form

*(Submit this completed form with your proposal submission. Fully complete a form for **each** proposed subcontractor. If a section does not apply, label it "not applicable." If the Respondent does not intend to use subcontractor(s), this form does not need to be returned.)*

Primary Respondent ("Primary Respondent"):	**AtlasIED**
Subcontractor Contact Information (individual who can address issues re: this RFP)	
Name:	**Mark Foerderer**
Address:	4545 East. Baseline Rd, Phoenix, AZ 85042
Tel:	**913-754-6096**
Fax:	**800-765-3435**
E-mail:	**mark.foerderer@atlasied.com**

Subcontractor Detail	
Subcontractor Legal Name ("Subcontractor"):	Atlas Sound LP
"Doing Business As" names, assumed names, or other operating names:	AtlasIED
Form of Business Entity (i.e., corp., partnership, LLC, etc.)	Limited Partnership
State of Incorporation/Organization:	Texas
Primary Address:	1601 Jack McKkay Blvd Ennis, TX 75119
Tel:	800-876-3333
Fax:	
Local Address (if any):	N/A
Addresses of Major Offices and other facilities that may contribute to performance under this RFP/Contract:	4545 East Baseline Road Phoenix, AZ 85042
Number of Employees:	300+
Number of Years in Business:	91
Primary Focus of Business:	Manufacturing
Federal Tax ID:	75-286 6896
Subcontractor's Accounting Firm:	Brunswick Benjamin P.C.
If the Subcontractor is currently registered to do business in Iowa, provide the Date of Registration:	N/A
Percentage of Total Work to be performed by this Subcontractor pursuant to this RFP/Contract.	N/A
General Scope of Work to be performed by this Subcontractor	
Detail the Subcontractor's qualifications for performing this scope of work	

By signing below, Subcontractor agrees to the following:

1. Subcontractor has reviewed the RFP, and Subcontractor agrees to perform the work indicated in this submitted Proposal if the Primary Respondent is selected as the winning Respondent in this procurement;

2. Subcontractor recognizes and agrees that if the Primary Respondent enters into a contract with the Agency as a result of this RFP, all restrictions, obligations, and responsibilities of the contractor under the contract shall also apply to the subcontractor;

3. Subcontractor agrees that it will register to do business in Iowa before performing any services pursuant to this contract, if required to do so by Iowa law; and,

4. Subcontractor certifies that it will comply with Davis-Bacon requirements if applicable to the resulting contract.

The person signing this Subcontractor Disclosure Form certifies that he/she is the person in the Subcontractor's organization responsible for or authorized to make decisions.

I hereby certify that the contents of the Subcontractor Disclosure Form are true and accurate and that the Subcontractor has not made any knowingly false statements in the Form.

Signature for Subcontractor:	*Mark Foerderer*
Printed Name/Title:	Mark Foerderer
Date:	12/15/25

Attachment #4 - Cost Proposal Template (also uploaded online)

The following has been entered into IOWA IMPACS via the JAEGGER Supplier Network portal. We are providing additional color via this appendix and including it for the reader's convenience.

Cost Category	One-Time Cost	Annual Cost	Quantity	Extended Total
System Licensing	$0.00	$49,500.00	1	$49,500.00
Equipment (camera, etc.)	included	included	NA	$0.00
Integration / Implementation	$2,270.00	NA	1	$2,270.00
Training (Initial)	included	Included	1	$0.00
Annual Support & Maintenance	included	Included	1	$0.00
System Upgrades / Enhancements	included	Included	1	$0.00

IntelliSee is priced as an inclusive **annual service** *indirectly* based on the number of camera streams monitored. IntelliSee sizes hardware requirements based on the number of camera streams which then determines the annual subscription cost. Hardware capacity range from monitoring as few as 10 camera views to monitoring 80+ views per appliance. Multiple appliances can be racked and seamlessly managed together. IntelliSee is continually evaluating larger servers and continued advancements in GPUs (the primary capacity constraint on the servers).

Pricing submitted via the JAEGGER Supplier Network portal is shown below but the following summarizes the costs associated with that submission:

- Software, hardware, and labor costs are based on the number of camera views listed in the "School District A" scenario (4 buildings, 870 students, 84 teachers, 90 cameras, etc.).
    - Camera counts translate to the size, quantity, and costs of the hardware required to monitor them which, in turn, drives monitoring subscription costs and configuration labor.
    - AI monitoring services - including IntelliSee's - monitor camera views. In most cases, there is a 1:1 camera to camera view ratio but some schools (and others) leverage 360-view cameras that contain four 90-degree streams. We are assuming this scenario does not contain multi-view cameras.
    - Iowa schools are on fiber optic so their camera networks are generally centralized (e.g. one network covering all of their buildings regardless of geographic location); This reduces hardware quantities (and cost) given bigger servers can be centrally located in data centers.
    - A theoretical district of this size (e.g. class 2A) likely has other locations that should be monitored as well - this includes administrative buildings, bus barns / operations centers, athletic facilities, childcare facilities, and so on. These can and should also be monitored by IntelliSee (the staff for these areas were not listed in the example).
- The IntelliSee license is extremely flexible:
    - Regardless of how much monitoring is purchased, they may load all cameras / camera views onto IntelliSee and toggle on / off camera views for monitoring (as long as they stay within the capacity limits of IntelliSee's hardware).

- IntelliSee does not cap the number of admins/users/alert recipients, enables administrators to make changes as needed, and does not charge separately for on-going support, maintenance, training, updates, and other costs others typically do.

- Related, IntelliSee is generally the highest value option available. It is often the most affordable option on its own but please ensure pricing is compared on complete basis.
  - IntelliSee includes all detection capabilities (e.g., trespassing, falls, etc.) and future upgrades - including new detection capabilities. As a result, customers have access to our entire AI safety platform for costs that are likely equivalent or lower than platforms that only help protect against active shooters (a very low probability event).
  - The IntelliSee platform enables customers to achieve an actual return on investment given the labor and prevention benefits associated with stopping other, more common incidents…all while also protecting against active shooter events.

IntelliSee is an Iowa-based company backed by the Iowa Economic Development Authority that formed specifically to help our schools and now others.

- To help support our Iowa schools and other public entities assisted by the Iowa Department of Management, we are offering additional discounts via this submission.
- As a sign of our commitment to the state and to our mission, we are reflecting an additional 10% discount off of annual monitoring costs for this RFP.

Due to all of the above, it is possible for "District A" in the example to protect its schools by monitoring its ~90 cameras for a total **first year cost of $51,770 and $49,500 annually thereafter.**

- This equates to ~$0.18 per student per day (or ~$0.16 per person per day when including staff) to protect the district from a litany of risks / threats they face.
- Given IntelliSee detects a broad and growing number of risks / threats, the cost per camera monitored per risk / threat detected per day is ~$0.17 per day. Substantially lower vs. systems that only monitor and detect drawn / brandished weapons.
- This cost per risk / threat monitored will continue to decline as IntelliSee adds more detection capabilities and as IntelliSee increases monitoring capacities (e.g. IntelliSee increased current customer monitoring capacity by ~25% earlier this year at no additional cost to customers).
- Beyond preventing active shooters, preventing a single common incident - e.g., a slip & fall claim, vandalism, etc. - generally pays for the entire IntelliSee system.
- IntelliSee users also experience labor savings, extend the life of their existing equipment / assets, and have other ancillary benefits which further increases their return on investment (ROI).

This proposal includes all necessary hardware, software, and labor to install a completely functional IntelliSee system. For the purposes of clarity, there are certain items and exclusions to note:

- IntelliSee AI appliances have rack-space, power, and bandwidth requirements that are very typical for standard data centers and surveillance camera networks. Racks, switches, network, and/or other data center or network enhancements are not included within this proposal.
- IntelliSee is an open platform designed to integrate with other systems. Labor to program downstream systems receiving IntelliSee alerts is not included within this proposal.

- IntelliSee is an AI company, not a camera or camera installation and service company. This proposal excludes any work related to an organization's cameras or camera network(s) beyond connecting cameras/networks to the IntelliSee visual intelligence platform.
- While IntelliSee is very flexible and can accommodate camera additions and other changes, this proposal excludes retrofitting IntelliSee to accommodate any subsequent changes to camera networks or other systems that would require fully reconfiguring the IntelliSee system.
- This proposal excludes work on other systems outside of this proposal.

IntelliSee also has **quantity discounts**, **prepayment discounts**, and **enterprise licenses** available that further reduce costs. Prices become even more attractive if customers take advantage of these options:

- Costs per camera drop dramatically as more camera streams are monitored by IntelliSee given fixed costs can be further spread.
- Prepaid multi-year contracts further enable IntelliSee to absorb fixed costs in exchange for being paid upfront.

Quantity discounts and prepayment discounts *enable customers to monitor an unlimited number of camera streams* with the associated purchase of the hardware needed. These approaches provide transparency into IntelliSee cost drivers and the flexibility to best meet their needs with that transparency.

For example, enterprise licenses give customers unlimited monitoring for a flat rate regardless of the number of camera views. The only incremental costs incurred are for any additional hardware and configuration costs associated with expanding monitoring beyond initial the capacity provided. These incremental costs are one-time expenses vs. the annual enterprise software license. One-time costs range from ~$6k to ~$20k depending upon the server sizes added.

Prepaid contracts provide substantial discounts to customers in exchange for the upfront payment. These generally are 3-year contracts and are often leveraged by school districts given they manage their financials from a cash flow perspective (vs. a P&L perspective used by private industry) and given many leverage safety grants. Prepaid 3-year contracts receive an equivalent discount of 50% off of one-year's monitoring (this roughly translates into the costs of IntelliSee's servers).

From a total cost perspective, the annual equivalent cost of ownership becomes very attractive if leveraging IntelliSee enterprise pricing and / or prepaid multi-year contracts. The net result is substantial savings opportunities within a platform that continuously improves, continuously adds capabilities, and that can continuously expand.

Attachment #5: Redlined Sample Contract (also uploaded)

Not applicable - no redlines

Attachment # 6: Exceptions to RFP & Contract Language (also uploaded)

Not applicable - no redlines

Terminations, Litigation, Debarment Document (also uploaded)

Terminations, Litigation, Debarment

The Respondent must provide the following information:

1. During the last five (5) years, has the Respondent had a contract for goods and/or services terminated for any reason? If so, provide full details related to the termination. None

2. During the last five (5) years, describe any damages or penalties or settlements to resolve disputes entered into by the Respondent under any of its existing or past contracts as it relates to goods and/or services performed that are similar to the goods and/or services contemplated by this RFP. If so, indicate the reason for the penalty or exchange of property, goods, or services and the estimated amount of the cost of that incident to the Respondent. None

3. During the last five (5) years, describe any order, judgment, or decree of any Federal or State authority barring, suspending, or otherwise limiting the right of the Respondent to engage in any business, practice, or activity. None

4. During the last five (5) years, list and summarize all litigation or threatened litigation, administrative or regulatory proceedings, or similar matters to which the Respondent or its officers have been a party. None

5. The Respondent must also state whether it or any owners, officers, or primary partners have ever been convicted of a felony. Failure to disclose these matters may result in the rejection of the Proposal or termination of any subsequent Contract. None

6. This is a continuing disclosure requirement. Any such matter commencing after the submission of a Proposal, and with respect to the successful Respondent after the execution of a Contract, must be disclosed in a timely manner in a written statement to the Agency. Agreed