NICE · Investigate
Overview for Businesses

DATE CREATED
19/04/2021

TABLE OF CONTENTS

NICE INVESTIGATE SOLUTION OVERVIEW

NICE Investigate is the industry's most comprehensive cloud-based solution for managing investigations and digital evidence, leveraging the ultra-secure Microsoft Azure Government cloud. NICE Investigate meets the FBI's rigorous CJIS (Criminal Justice Information Services) requirements. It has earned the CJIS ACE Compliance Seal from Diverse Computing for NICE Investigate following a rigorous 553-point review of the solution.

NICE Investigate automates and speeds up the entire evidence collection, discovery, analysis, management, notification and sharing process. It improves productivity by eliminating manual, time consuming evidence collection and analysis activities, ultimately helping investigators close more cases faster. Investigators can now spend less time gathering and organising evidence, checking and rechecking to ensure they have everything and have more time for investigating. Prosecution is able to be certain they have all evidence for trial that is available and are immediately notified when there is new evidence so they can invest their time in trial strategy and formulating legal arguments for successful prosecutions.

NICE Investigate is the only end-to-end solution to address digital evidence management challenges through the complete life-cycle of an investigation. It does it through three innovative application portals: the Community Portal, the Investigation Portal, and the Prosecution Portal.

By centralising access to information and standardising processes through predefined workflows, NICE Investigate Portals promote tighter collaboration among communities, satellite agencies, investigators and prosecutors. This enhances the effectiveness of law enforcement, while tracking continuity of evidence as it is collected, organised and distributed. It also encourages the adoption of consistent, repeatable, efficient processes.

Community Portal

NICE Investigate's Community Portal is a channel for community engagement and evidence collection through crowdsourcing. Citizens can submit tips and upload evidence securely, such as cell phone photos and videos. In the Community Portal businesses can also register their CCTV cameras along with their contact information and camera location, empowering investigators to easily identify recorded zones in a crime scene investigation.

The cameras are then geo-located on a map within NICE Investigate so investigators can get an instant view of which cameras are in the area of a crime scene, without having to physically canvas the area on foot. With NICE Investigate, they can request a copy of the video directly.

Evidence gathering from the community no longer causes delayed case resolution.

Investigation Portal

The Investigation Portal is the primary workspace for investigators. This is where they organise, analyse and interpret evidence, and build their cases and share them.

The Investigation Portal provides a one-stop location for automatically gathering evidence from all connected digital evidence data silos. A powerful 'Google-like' search function allows investigators to conduct a single search to uncover hidden evidence and connections, and bring back evidence from all connected structured and unstructured data sources—including databases, narratives from CAD comments, incident reports, FI cards, reports and documents, and much more.

With the Investigation Portal, investigators can request any information that is not readily available, such as CCTV footage from businesses or call recordings from 911 communication centres, or the enhancement of a digital photograph or a specific test on a collected piece of evidence. Investigators can initiate and track evidence requests using built-in workflows.

Investigators as well as others that choose to follow a case can be notified when an evidence request is fulfilled or when new evidence is added to their cases. Now that NICE Investigate breaks down the barriers between information silos and keeps investigators informed about emerging evidence, investigators are no longer likely to overlook a crucial piece of evidence in a case.

But collecting digital evidence is just the beginning. NICE Investigate also solves the challenge of putting all the pieces of evidence into context based on time sequence and location. There could be hours of video footage, numerous audio recordings, physical evidence, and stacks of crime scene photos associated to a case. With NICE Investigate, investigators no longer spend gruelling hours manually sifting through all the evidence trying to

make sense of it. NICE Investigate synchronises and visualises everything in maps and on timelines, which is particularly valuable for officer pursuit, use of force, homicides and large-scale incident reviews.

By visualising all existing evidence, uncovering new relevant evidence, and helping Investigators analyse all of it in useful ways, NICE Investigate can help investigators start their investigation sooner and get to case resolution faster. .

Prosecutor Portal

The Prosecutor Portal is NICE Investigate's prosecutor access point that eliminates the need to hand-deliver digital evidence. Prosecutors receive an email with a link to the digital case files with all the related information (or specific items in a case)—Investigate provides receipts and tracks who sees what data and when. Evidence admissibility is ensured through automated chain of custody tracking and reporting. Prosecutors can also share evidence through Investigate to the defence in an electronic form eliminating the need to make copies of evidence.

Historically, police reports and crime scene photos arrived at courthouses in multiple boxes, and more recently on thumb drives or compact-discs. The disjointed nature of the evidence can diminish its prosecutorial value. It's very difficult for a prosecutor to piece together a coherent timeline from dozens of files copied onto CDs, DVDs, and thumb drives. Lacking the benefit of the investigator's analysis, the prosecutor has to wade through the materials on his or her own. Through the Prosecutor Portal, prosecutors can visualise evidence in meaningful ways, for example on maps and timelines. They can play back video recordings and view images side by side to gain a complete understanding of events leading up to and following the incident under investigation. Now they can collaborate more effectively with police investigators as they build their cases.

NICE INVESTIGATE CAPABILITIES OVERVIEW

The following sections provide an overview of the NICE Investigate capabilities that are provided as a part of this solution and the specific challenges that these elements of NICE Investigate are designed to address.

The functionality described includes:

Comprehensive Collection of Evidence

- From all connected systems via automated processes
- Public Appeals and Crowdsourcing evidence captured by citizens
- Online uploads of CCTV camera video by businesses
- Manual uploads by investigators or 3rd parties
- Community Portal

Secure, Centralised Access to Evidence

- Secure user login from virtually anywhere
- Roles-based access rights
- Automated audit logs

Efficient Case and Evidence Analysis

- Investigator Portal
- User-friendly case and evidence views
- Automated synchronisation and visualisation of evidence on maps and timelines
- Rapid searches through all evidence types
- Intelligent evidence suggestions
- Advanced video management

Instant Sharing of Case Evidence with Prosecution

- Prosecutor Portal
- 3rd party User and Device Management
- Tracking share activity

Automated Workflows Assure Consistency and Operational Efficiency

- Auto-collection of evidence from integrated systems
- Management of security – virus scans, encryption, chain of custody activity logs
- Organisation of evidence into case folders
- Notifications to assure that all investigators are aware of the latest evidence added to their cases
- Evidence requests
- Case and evidence sharing
- Chain of custody tracking to assure admissibility of evidence in courts

Administration and Solution Architecture

- Administrator Portal
- Bandwidth and storage requirements
- IT benefits

NICE INVESTIGATE AUTOMATED EVIDENCE COLLECTION

NICE Investigate is uniquely designed to automate and streamline what all too often are manual and physical steps for officers today, as they collect digital evidence items from multiple disconnected places, directories, databases and content management systems of any combination of vendor solutions.

As shown in the following diagram, a NICE Investigate Data Source Gateway (DSG) software appliance connects to a police department's existing evidence capture platforms and storage locations and automates the collection process to bring all evidence tagged with valid case related identifiers into a centralised storage repository in Investigate.

Digital evidence items along with all of their associated metadata are securely uploaded without any need for user intervention. This approach saves time and improves the accuracy of the data collected, while also improving the efficiency and effectiveness of every investigator.
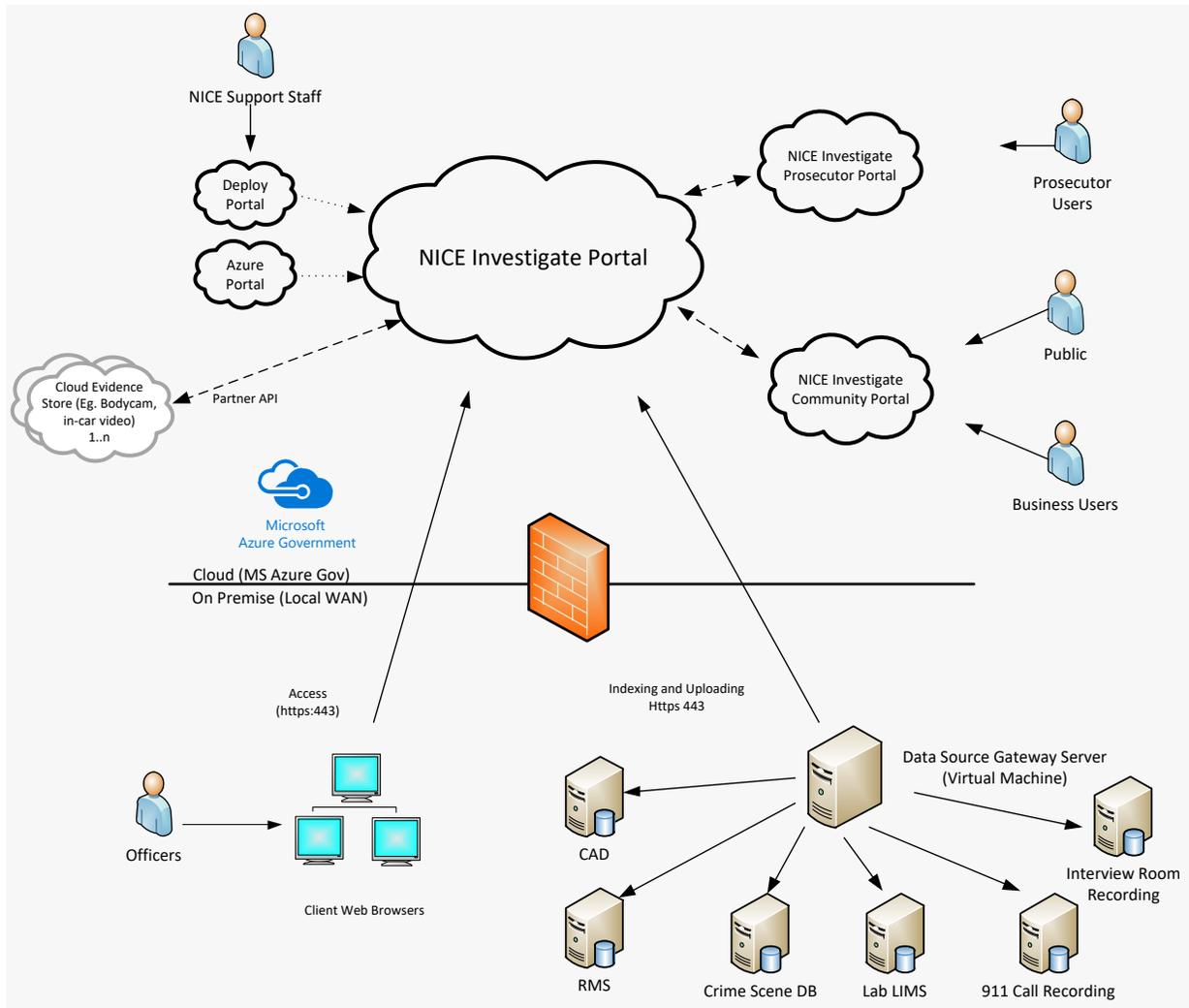
Figure 1: **The NICE Data Source Gateway**

NICE INVESTIGATE WORKFLOWS FOR EVIDENCE COLLECTION

Investigators invest a significant amount of time and resources into locating and collecting information not only from within the department but also from the public. Too often, locating and collecting evidence demands time spent driving, phoning and emailing and once the information is finally obtained, duplicating DVD's.

With NICE Investigate, workflows can be set up to help users manage the collection and processing of evidence through consistent, repeatable, agency-approved processes. Your investigators, officers, and other authorised personnel can initiate workflow requests through NICE Investigate; the system tracks and logs all requests and automatically notifies the investigator (or another designated user) when those requests have been fulfilled.

Following is a list of default Investigate Workflows.

- Initiate a request for CCTV video footage

- Initiate a request for evidence to a person associated with an Investigation

- Initiate a Public Appeal for information related to an incident

- Initiate a Request for Evidence from another department

Additional workflows can be added to meet your organisations specific needs. Examples of other workflows could include:

- Initiate a request for evidence processing from another department or agency (e.g. forensic crime lab)

- Initiate a request for evidence from another agency

- Initiate a request for a follow up (interview someone, collect evidence, etc.)

Initiate a Request for CCTV video footage

An Investigate user can rapidly locate and request CCTV footage from businesses who have registered their cameras with the Police via the NICE Investigate Community Portal.

The Investigate user can choose one or multiple cameras in their map view and initiates a workflow that sends an email to the registered owner(s) of the camera(s) with a link to the request. The registered owner(s) is able to click on the request link, securely log in to the NICE Investigate Community Portal and view the request details interface. The owner is then able to upload requested video.

Once uploaded, the Investigate user is notified that the request has been completed and is able to go to the request view within their case to see the uploaded material and can choose to add to the Investigate evidence folder for their case.
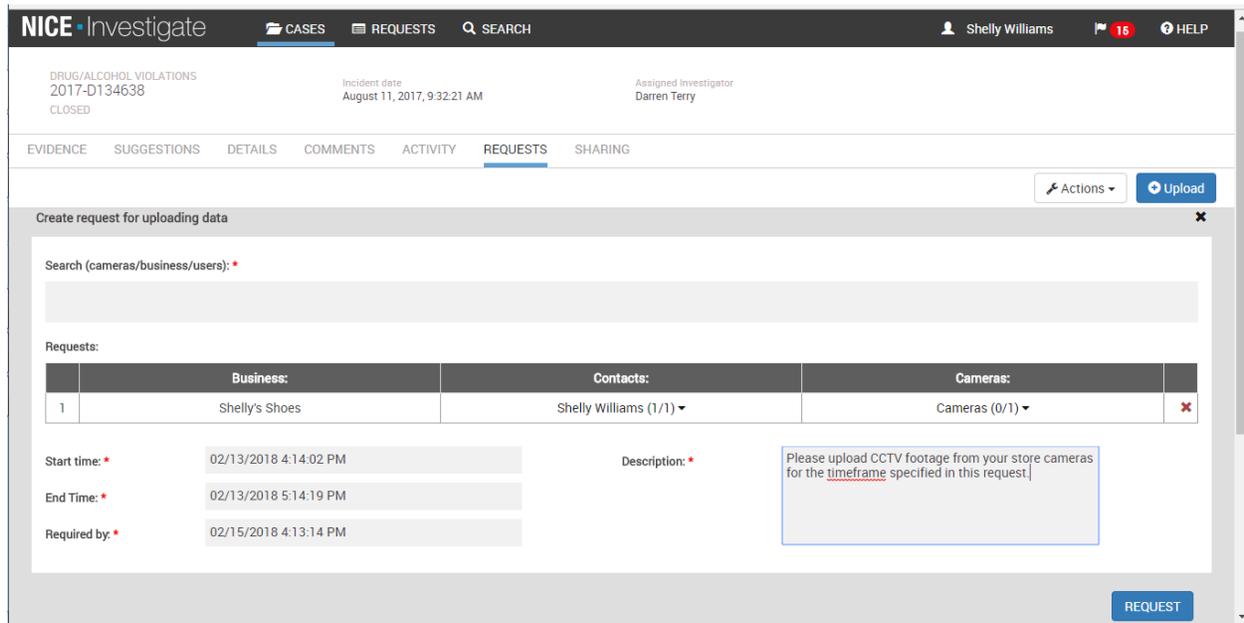

Figure 2: **Initiate a CCTV Video Request**

NICE INVESTIGATE SECURE EVIDENCE MANAGEMENT

NICE Investigate provides a baseline set of security controls providing appropriate protection against typical threats such as unauthorised access to the service; upload of malicious content to Investigate; unauthorised access and distribution of assets in Investigate.

All information is handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.

- Hosted in the Microsoft Azure Government data centres. This cloud platform and application are CJIS certified and provide enhanced security policies for access control and maintenance.
- Encryption at rest of all collected digital evidence along with any metadata using strong AES-256 encryption.
- Virus checking of all data uploaded to Investigate to protect against malicious content being uploaded.
- User access is via secure HTTPS browser connections with 2-factor authentication for login
- Attribute based access controls for accessing digital evidence
- Chain of custody reports proving the authenticity of collected evidence

Following is a schematic that illustrates how data is secured within the Azure Government network. It shows the agency secure areas and the Microsoft Azure Government cloud secure areas with encrypted data transfer between them.

In addition, public and community-generated data (e.g. crowdsourced data or uploaded third party video) is stored in the Microsoft Azure public cloud, and is virus scanned before it's transferred to the Microsoft Azure Government cloud. This ensures that all information entering the Microsoft Azure Government cloud is virus-free and doesn't pose a danger to the secure system.

In the NICE Investigate solution architecture shown below, the coloured rectangles are secure and the blue interconnects are encrypted.
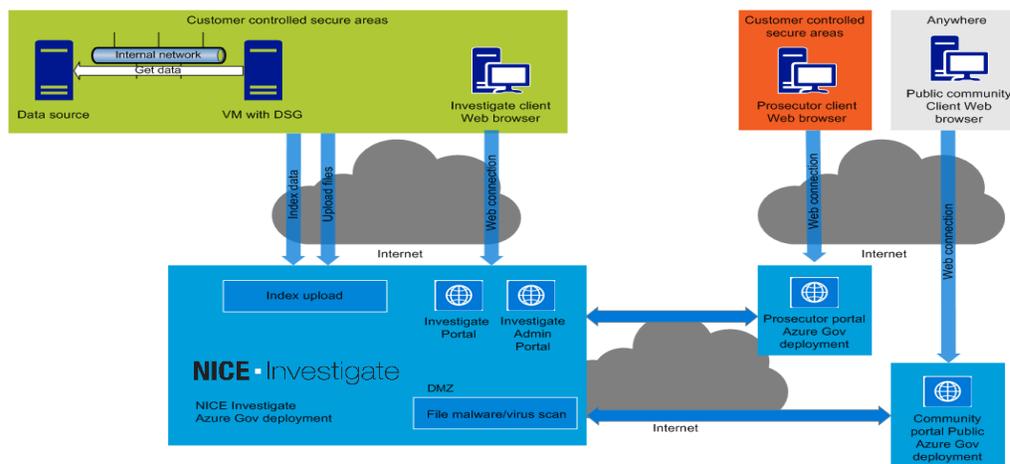
Access to Evidence

NICE Investigate implements an attribute based access control (ABAC) framework, where access rights are granted to users through the use of policies that combine attributes. This provides a robust set of capabilities to ensure access to information is ONLY granted on the basis of a genuine "need to know".

The control of access rights are established in Investigate via access rules that are implemented to ensure users, user groups, and administrators are only provided with access to data and platform capabilities that are required for their role.

It is also possible to create a connection to synchronise and inherit access control rules with a customer's existing records management system as a custom integration.

The NICE Investigate System Administrator is responsible for working with the NICE system engineer to implement access rules for users.

The System Administrator may grant, change or revoke access rights either manually or via an approved role-based enforcement solution. The System Administrator has the ability to deactivate a user account, or to assign a user to another group or role in Investigate.

NICE INVESTIGATE SECURITY EVIDENCE MANAGEMENT ENSURES DATA IS SAFE AND ACCESS IS GRANTED ONLY TO THOSE WITH A NEED TO KNOW.

NICE INVESTIGATE AUDIT LOGS AND CHAIN OF CUSTODY

A comprehensive system audit log tracks all activity in NICE Investigate. This includes platform-generated activity, user-generated activity, and system administration activity. Each audit entry includes information on who completed the action and when the action occurred, along with any additional details associated with the action. Unsuccessful attempts are also audited.

Audit Logs provide information on platform-generated activity such as automated upload of evidence to an Investigate case folder, virus checking, security hash activity, and creation of transcoded copies of evidence items. Logged user activity includes accessing a digital evidence folder, viewing digital evidence items, creating or modifying evidence metadata, uploading, sharing, downloading digital evidence items, etc.

Audit logs are read-only in NICE Investigate. Each NICE investigate user has access to case and evidence audit logs and chain of custody reports for their assigned cases. There is also a master audit log that has information on all system activity across all users. The master log is accessible via the NICE Investigate Administrator portal. Access to this master audit log is privilege controlled.

The authenticity of audit records is ensured by the use of a hash chaining mechanism (the audit records/blocks are linked and secured using cryptography). The chaining of blocks uses HMAC-256 and employs a 256-bit salt.

Chain of custody reports are created from the evidence collected in the NICE Investigate audit logs. These chain of custody reports provide proof of the authenticity of the collected evidence and can be sent alongside digital evidence when shared with the prosecution and others for court purposes.

Audited Case Activity includes:
- When a case is created
- When a case is accessed by a user
- When case details (metadata) are modified by a user
- When a case is downloaded by a user
- When a case is shared by a user
- When case access is granted/revoked by a user

Audited Evidence Activity includes:

- When evidence is uploaded to Investigate
- When evidence virus check is completed
- When evidence hash is created/signed
- When evidence working copy is created
- When evidence is accessed by a user
- When evidence details (metadata) are modified by a user
- When an evidence clip/snapshot is created
- When an evidence redaction is created
- When evidence bookmarks/comments are added
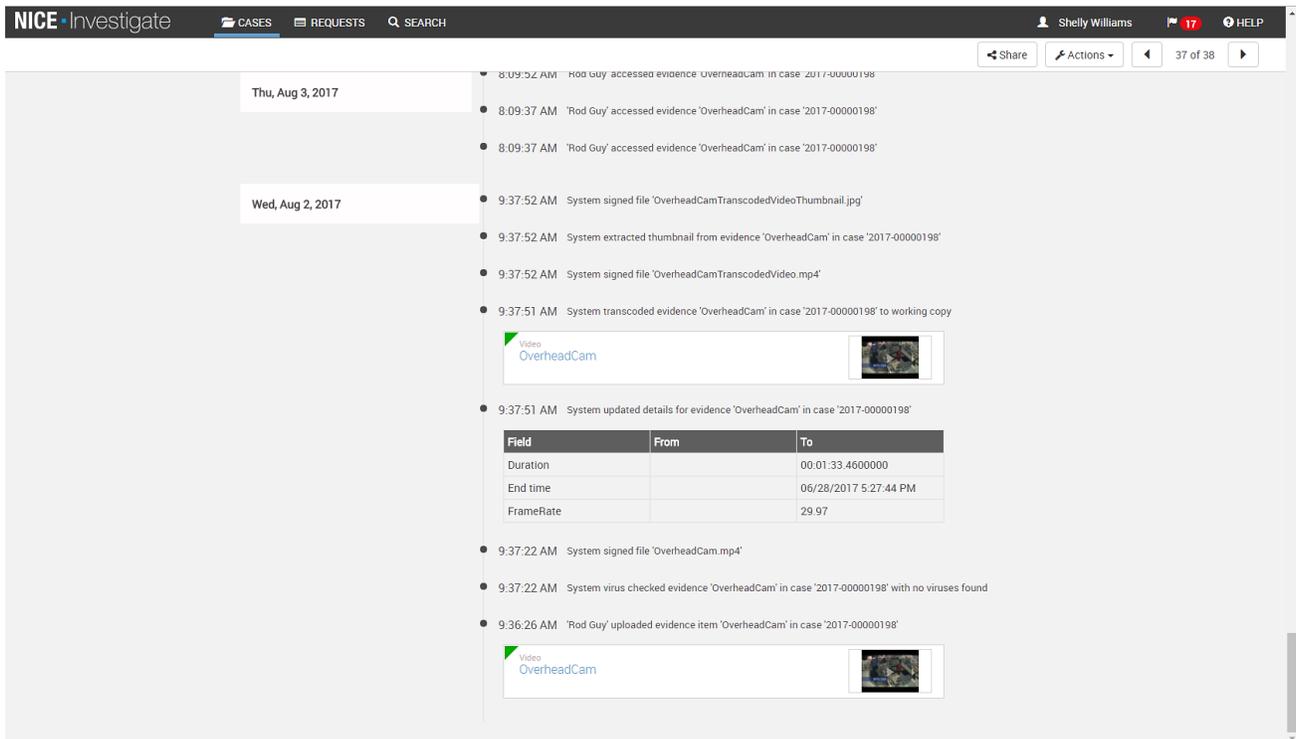- When evidence is downloaded by a user
- When evidence is shared by a user

Figure 3: **Activity and Chain of custody logs**

NICE INVESTIGATE AUDIT LOGS ENSURE CHAIN OF CUSTODY AND PROVIDES THE USER A METHOD FOR SUBSEQUENTLY VERIFYING THE AUTHENTICITY OF EACH DIGITAL EVIDENCE ITEM.

NICE INVESTIGATE EVIDENCE RETENTION POLICIES

NICE Investigate can automatically manage evidence retention based on predefined rules. Retention rules can be based on can be set based on any metadata characteristic or a combination of characteristics of an evidence item. Two of the most common parameters used to create retention rules include:

- The type of case – Digital evidence can inherit the retention category that is assigned to a given case as obtained from metadata collected from the connected CAD or RMS. For example, a police

department can set retention rules based on case incident type and set retention for burglary cases to be 5 years, homicide cases to be retained forever, etc. All digital evidence items within a burglary case will inherit the 5 year retention rule unless overridden manually (by an authorised user).

- The type of evidence –An evidence item type such as crime scene photos, body camera recordings, etc. can have a pre-defined deletion date such as 'x' months, once defined as a rule.

Once the retention rules are defined and updated in NICE Investigate, all evidence, upon upload to Investigate is assigned a retention category. Storage of an evidence item is then managed based on the assigned retention category and an appropriate deletion date is set.

Reviews and approvals for deletion can be included as a part of any retention policy set in NICE Investigate. Prior to the deletion of an evidence item, a retention policy can be configured to send a deletion approval notice to a designated user who then has the ability to review and approve the deletion or extend the retention period of the evidence item as needed. The evidence item will only be deleted when the approval is provided.

If a mistake is made and an evidence item is deleted in error, the Investigate System Administrator can retrieve the evidence item from the Investigate "regret bucket". This "regret bucket" for deletions has a timeframe of 'xx' days as configured by the Investigate System Administrator. Once 'xx' days have passed, a digital evidence item is permanently deleted from the system and cannot be retrieved.

INVESTIGATE RETENTION POLICIES ALLOW FOR WORRY-FREE, AUTOMATED MANAGEMENT OF EVIDENCE DELETION POLICIES. PROACTIVE DELETION APPROVAL NOTIFICATIONS ENSURE PROPER OVERSIGHT AND REVIEW.

NICE INVESTIGATE COMMUNITY PORTAL

The NICE Investigate Community Portal provides citizens and businesses with a way to share tips, photos and video with a Police Agency.

The NICE Investigate Community Portal is designed to ingest potentially massive quantities of media from the public (including video from cameras, smartphones, etc.) to assist in the investigation of a major incident or day-to-day crime activity.

The Community Portal consists of two portal user interfaces and can be personalised and made available via an agency's existing web presence for access by citizens and businesses.

The Community Portal Business Interface enables businesses and citizens to register their contact information and surveillance camera systems and with a Police Department.

Registered camera systems are geo-located on the NICE Investigate map view and presented alongside case and evidence data for Investigate users to visually see registered camera sources that may be nearby to an incident. Investigate Suggestions also highlight nearby camera sources for Investigate Cases.

Once registered, businesses and citizens are able to receive electronic requests for evidence from the Police Department. Requested data can be uploaded directly to the Community Portal Business interface to be securely delivered back to the requesting officer.

NICE Investigate Community Portal Capabilities for registered users Include

- Register account contact information

- Set up username and password
- Register and Manage Camera Sources
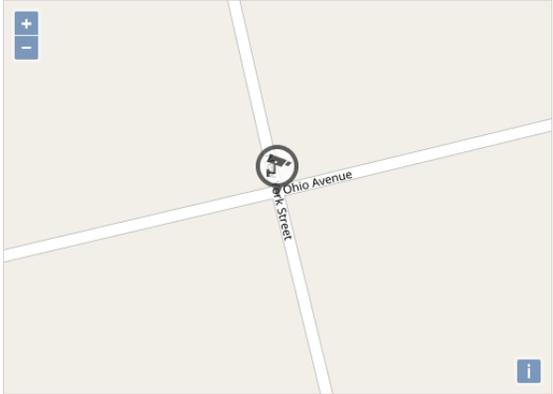- View and respond to Police Requests

Figure 4: **Community Portal Requests view**

Figure 5: **Community Portal Camera Registration View**