NACA 2026

Competency Framework

for Crime Analysis

Core skills, knowledge domains, proficiency standards, and ethical requirements for the crime analysis profession.

National Association of Crime Analysts (NACA)
Advocacy & Standards Division | 2026 | naca-usa.org

Introduction and Purpose

The NACA National Competency Framework defines what it means to be a competent crime analyst. It is the authoritative reference for the profession - establishing the skills, knowledge areas, and ethical standards that should guide hiring decisions, job classification, performance evaluation, training investment, and career development across all agency types and sizes.

This framework is explicitly focused on crime analysis: the data-intensive, technically grounded discipline of turning law enforcement data into actionable information that drives operational decisions. It does not describe intelligence analysis, criminal investigation, or law enforcement operations generally. Crime analysts are data professionals, and this framework reflects that reality.

> **WHO THIS FRAMEWORK IS FOR**
>
> Crime analysts at all career stages are seeking a clear map of professional expectations. HR departments and civil service bodies, who are setting or updating analyst job classifications and pay grades. Police chiefs and administrators are evaluating analyst staffing needs and performance. Training providers and academic programs are designing curricula that reflect genuine professional requirements.

Framework Structure

The framework is organized into six competency domains, each containing a set of skill areas with defined proficiency levels. Every crime analyst is expected to demonstrate competency across all six domains - depth and specialization will vary by role, agency size, and career stage. An analyst focused primarily on tactical crime series work, for example, may show deeper proficiency in Domains 3 and 4, while an analyst supporting data infrastructure and reporting may show deeper proficiency in Domains 1, 2, and 5. This framework describes the full range of competencies the profession covers, not a uniform expectation that every analyst reach the same depth in every domain, though every analyst is still expected to build competency in all five. New analysts especially should read this as a roadmap for where to grow.

#	Domain	Core Focus
1	**Data Fundamentals & Literacy**	SQL, data structures, data quality, database systems

2	**Data Management & Infrastructure**	System integration, governance, and semantic modeling
3	**Spatial Analysis & Mapping**	GIS, hot spot methods, geographic data management
4	**Statistical Analysis & Pattern Recognition**	Descriptive stats, trend analysis, and crime series identification
5	**Automation, Reporting & Visualization**	Dashboards, automated workflows, data storytelling
6	**Professional Practice & Ethics**	Legal frameworks, analytical integrity, and communication

Proficiency Levels

Each skill area within the six domains is rated at one of three proficiency levels. These levels are used to distinguish entry, mid-career, and senior analyst expectations, and to guide hiring rubrics and performance evaluations.

Level	Foundational	Proficient	Advanced
Definition	Understands the concept; can perform with guidance or reference materials	Performs independently and consistently; applies to novel situations	Leads, teaches, or designs systems in this area; handles edge cases and complexity
Typical career stage	Entry-level (0–2 years)	Mid-career (3–6 years)	Senior / Lead (7+ years)
Expectation	Demonstrates awareness; completes supervised tasks	Owns the function; produces reliable outputs	Mentors others; builds institutional capacity

DOMAIN 1 · Data Fundamentals & Literacy

Data literacy is the foundational competency of the crime analysis profession. Before any analysis, mapping, or reporting can occur, analysts must understand how law enforcement data is structured, where it comes from, what it means, and how it can fail. This domain covers the technical and conceptual skills required to work with data at a professional level.

1.1 SQL and Database Querying

SQL (Structured Query Language) is the primary tool by which crime analysts extract, filter, join, and aggregate data from relational databases - including RMS (Records Management Systems), CAD (Computer-Aided Dispatch), jail management systems, and other law enforcement data stores. SQL proficiency is non-negotiable for any analyst working in a data environment.

Skill	Foundational	Proficient	Advanced
SELECT / WHERE / ORDER BY	Writes basic single-table queries with filtering and sorting	Writes multi-condition queries with calculated fields and aliases	Optimizes queries for performance; understands query execution plans
JOINs (INNER, LEFT, etc.)	Understands join concepts; performs guided joins	Independently joins multiple tables; troubleshoots mismatched keys	Designs normalized schemas; advises on join strategy for complex data models
Aggregation (GROUP BY, COUNT, SUM, AVG)	Performs simple counts and sums	Builds multi-level aggregations with HAVING clauses	Creates aggregation pipelines; uses window functions
Subqueries & CTEs	Reads and modifies existing subqueries	Writes subqueries and CTEs independently	Refactors complex queries using CTEs for readability and performance
Date/Time functions	Extracts year, month, day from date fields	Calculates time differences; filters by date ranges	Handles timezone offsets, fiscal periods, shift-boundary edge cases
Data export for analysis tools	Exports query results to CSV/Excel	Parameterizes exports for recurring pulls; schedules queries	Builds automated export pipelines to BI tools or Python/R environments

Table 1.1: SQL proficiency matrix

1.2 Understanding Law Enforcement Data Structures

Crime analysts work with a specific ecosystem of data systems. Understanding how these systems are built, what fields they contain, how records are created, and where data quality problems typically arise is essential before any analytical work can be meaningful.

- Records Management Systems (RMS): offense reports, arrest records, field contacts, case management
- Computer-Aided Dispatch (CAD): call-for-service records, unit assignments, response times, disposition codes
- Jail Management Systems: booking data, charges, release dates, custody status
- Citation and traffic systems: moving violations, accident reports, DUI data
- External data feeds: parole/probation status, sex offender registry, court disposition data, open source intelligence (OSINT), and commercial location data sources
- Field data: body-worn camera metadata, officer-initiated activity logs

WHY THIS MATTERS

An analyst who does not understand how CAD disposition codes are assigned or how an RMS incident type differs from an arrest charge will produce analyses that appear valid but reflect data-entry conventions rather than ground truth. Understanding the provenance of every data field is a professional requirement, not an advanced skill.

1.3 Data Quality Assessment and Validation

Law enforcement data is inherently imperfect. Officers enter data under pressure, systems have field validation gaps, and conventions change over time. Analysts are responsible for understanding and communicating data quality limitations in every product they produce.

Skill Area	Foundational	Proficient	Advanced
Missing data identification	Flags NULL/blank fields in query results	Quantifies completeness rates; identifies patterns in missing data	Designs data quality dashboards; traces missingness to source systems
Duplicate detection	Identifies obvious duplicate records manually	Writes queries to detect duplicates using key field combinations	Builds deduplication rules; manages merge/purge workflows
Geocoding quality	Understands geocoding success vs. failure rates	Reviews and corrects geocoding failures;	Manages geocoding pipelines; establishes agency address standards

		assesses address standardization	
Temporal consistency	Checks for obviously wrong dates (future dates, impossible times)	Validates event sequences (report time after occurrence time)	Audits shift-boundary data entry patterns; flags systematic recording delays
Communicating limitations	Notes data caveats in reports when prompted	Proactively includes data quality notes in all analytical products	Writes formal data quality documentation; advises command on data reliability

Table 1.3: Data quality proficiency matrix

1.4 Data Literacy and Interpretation

Data literacy, the ability to read, understand, and critically evaluate data-based claims, is both a skill analysts must possess and a capability they are responsible for building across their agencies. Analysts serve as the data literacy resource for their departments.

- Understanding the difference between counts, rates, and ratios, and knowing when each is appropriate
- Recognizing when a change in data reflects a real-world change versus a recording artifact, policy change, or system migration
- Explaining data concepts to non-technical audiences: commanders, city councils, and media
- Critically evaluating data visualizations and statistical claims produced by vendors, consultants, or other agencies
- Understanding base rates and their effect on comparisons across agencies, time periods, and geographies

DOMAIN 2 · Data Management & Infrastructure

Crime analysts do not merely consume data; they build and maintain the systems through which their agencies collect, store, and use it. This domain covers the infrastructure, governance, and semantic modeling work that makes data usable at the organizational level.

2.1 Database Design and Management

Skill Area	Foundational	Proficient	Advanced
Relational database concepts	Understands tables, primary/foreign keys, basic normalization	Designs normalized schemas for analytical use cases	Architects multi-source data warehouse structures for agency-wide use
Database platform proficiency	Navigates and queries existing databases (SQL Server, Access, PostgreSQL, MySQL)	Creates, modifies, and maintains tables, views, and stored procedures	Manages database administration tasks; optimizes for query performance
Data import/ETL processes	Imports structured files (CSV, Excel) into a database manually	Builds repeatable ETL workflows for recurring data ingestion	Designs automated ETL pipelines with error handling and logging
Data retention and archiving	Understands agency retention policies	Implements archiving workflows that comply with retention schedules	Develops and documents agency data lifecycle policies

Table 2.1: Database management proficiency matrix

2.2 Semantic Modeling

Semantic modeling is the practice of defining what data means, how fields relate to one another, and how information should be structured for reliable use across different systems, roles, and analytical contexts. It is among the most consequential and least formally recognized functions crime analysts perform.

- Building data dictionaries that define every field in agency data systems: what it means, how it is populated, what values are valid, and how it has changed over time

- Creating and maintaining taxonomies for incident types, offense categories, disposition codes, and geographic zones, ensuring consistent terminology across units and reporting periods
- Developing semantic layers in BI tools (Power BI, Tableau, Qlik, etc.) that translate raw database fields into named, business-logic-aware measures and dimensions
- Designing calculated fields, KPIs, and derived metrics that reflect agency-specific definitions, not default vendor assumptions
- Documenting the logic behind analytical products so that reports can be reproduced, audited, and handed off across staff transitions
- Reconciling terminology differences between systems (e.g., where RMS and CAD use different codes for equivalent events) into unified analytical categories

THE SEMANTIC LAYER AS INSTITUTIONAL MEMORY

Every data definition an analyst builds and documents is institutional knowledge that survives staff turnover. Agencies without formal semantic layers risk losing analytical continuity each time an experienced analyst departs. Building and maintaining this layer is not administrative overhead; it is infrastructure with a long organizational life.

2.3 System Integration and Data Governance

- Understanding data-sharing agreements and the legal/policy frameworks that govern inter-agency data exchange
- Managing data feeds from external systems: parole/probation, regional fusion centers, state repositories, federal databases
- Establishing and enforcing data entry standards that improve the quality of data collected at the source (officer level)
- Participating in RMS/CAD procurement and configuration processes to ensure analytical requirements are represented
- Documenting data lineage, where each data element originates, how it is transformed, and where it ends up in analytical products

DOMAIN 3 · Spatial Analysis & Mapping

Spatial analysis is a defining competency of crime analysis. The ability to translate crime data into geographic representations, and to apply spatial methods that identify concentration, displacement, and environmental risk factors is one of the most visible and operationally valuable outputs analysts produce.

3.1 GIS Fundamentals

Skill Area	Foundational	Proficient	Advanced
GIS platform proficiency	Navigates ArcGIS or QGIS; opens layers, uses basic symbology	Creates, edits, and publishes maps; manages layer files and projects	Builds and maintains enterprise GIS environments; manages geodatabases
Geocoding	Geocodes addresses using existing services; understands match rates	Manages geocoding workflows; troubleshoots failures; improves match rates	Designs geocoding pipelines with address standardization and fallback logic
Coordinate systems & projections	Understands that projections exist; uses projected layers correctly	Reprojects data; selects appropriate projections for local analysis	Manages projection libraries; advises on coordinate system standards for agency data
Spatial joins and overlays	Performs point-in-polygon joins with guidance	Independently performs spatial joins, clips, and intersects	Designs multi-layer spatial analysis workflows for operational products
Layer management	Opens and displays existing layers	Organizes, symbolizes, and documents layer files	Maintains agency layer library; manages shared GIS resources

Table 3.1: GIS fundamentals proficiency matrix

3.2 Hot Spot Analysis and Crime Concentration Methods

Hot spot analysis is the application of spatial statistical methods to identify geographic concentrations of crime. Analysts must understand both the technical execution of these methods and the operational limitations of each approach.

Method	What Analysts Must Know
Kernel Density Estimation (KDE)	How bandwidth selection affects output; difference between KDE and point maps; interpreting density surfaces for patrol deployment
Spatial Ellipses / STACs	How to construct and interpret standard deviational ellipses; use in crime series deconfliction and series tracking
Grid-based analysis	Cell size selection and its effect on interpretation: using grid counts for repeat address analysis
Near-Repeat Analysis	The near repeat victimization concept[1]: using NR analysis to generate predictive patrol recommendations with appropriate caveats
Choropleth mapping	Appropriate use of rate vs. count maps; classification scheme selection; communicating geographic comparisons honestly

Table 3.2: Hot spot and spatial analysis methods

3.3 Operational Mapping Products

Beyond analytical maps, crime analysts produce operational mapping products - formatted, audience-specific documents designed to drive immediate action by patrol, command, or administrative audiences.

- Patrol deployment maps: geographically bounded, time-filtered, operationally actionable - not raw data dumps
- Crime series maps: tracking linked offenses across time with suspect/vehicle information integrated
- Beat and sector analysis maps: supporting boundary design, workload comparisons, and staffing decisions
- Community briefing maps: simplified, clearly labeled, appropriate for public or city council audiences
- Grant and reporting maps: meeting federal and state reporting standards for geographic data

[1] Near-repeat victimization was first identified by Townsley, Homel, and Chaseling (2003) and developed further by Johnson and Bowers (2004), who found that proximity to a recent crime elevates risk at nearby locations for a limited window of time. See Townsley, M., Homel, R., & Chaseling, J. (2003). "Infectious burglaries: A test of the near repeat hypothesis." *British Journal of Criminology*, 43(3), 615–633; Johnson, S. D., & Bowers, K. J. (2004). "The stability of space–time clusters of burglary." *British Journal of Criminology*, 44(1), 55–65.

DOMAIN 4 · Statistical Analysis & Pattern Recognition

Crime analysts are applied statisticians. They must be capable of producing statistically sound analyses of crime data, communicating uncertainty appropriately, and recognizing the difference between meaningful patterns and statistical noise. This domain covers quantitative methods as applied specifically to law enforcement data.

4.1 Descriptive Statistics and Data Summarization

Skill Area	Foundational	Proficient	Advanced
Measures of central tendency	Calculates mean, median, mode; knows when each is appropriate	Selects appropriate measures for skewed distributions; explains to non-technical audiences	Advises on aggregate measure choice for agency KPI design
Measures of dispersion	Understands range and standard deviation conceptually	Calculates and interprets standard deviation and IQR in crime data	Uses dispersion measures to set alert thresholds and detect anomalies
Frequency distributions	Creates frequency tables and histograms	Interprets distributional shape; identifies outliers	Fits distributions to crime data; uses for simulation and forecasting
Cross-tabulation	Creates two-variable crosstabs	Builds multi-variable tables; calculates row/column percentages correctly	Designs cross-tab logic for automated reporting systems
Time-of-day / day-of-week analysis	Produces counts by hour and day	Creates shift-adjusted temporal profiles; distinguishes reporting patterns from crime patterns	Builds temporal baseline models for anomaly detection

Table 4.1: Descriptive statistics proficiency matrix

4.2 Trend Analysis and Forecasting

- Calculating percent change correctly, and knowing when percent change is misleading (small base numbers, year-over-year vs. period-over-period)

- Applying moving averages and smoothing techniques to reduce noise in weekly or monthly crime counts
- Distinguishing statistically meaningful trend changes from normal variation using control chart methods (upper/lower control limits)
- Seasonal adjustment: identifying and accounting for seasonal crime patterns when comparing across months or years
- Communicating forecast uncertainty: analysts produce informed projections, not predictions, and must convey confidence intervals appropriately

4.3 Crime Pattern and Series Recognition

Pattern recognition is the identification of structurally linked criminal events, events that share sufficient characteristics (method, target, geography, timing) to suggest a common offender, group, or environmental driver. This is a core analytical function distinct from intelligence analysis, rooted in data comparison rather than source development.

Pattern Type	Definition	Analyst Responsibility
Crime Series	Multiple offenses were likely committed by the same individual or group	Link analysis across offense reports; MO comparison; geographic and temporal clustering; timeline reconstruction across linked incidents
Crime Pattern	Multiple offenses sharing geographic, temporal, or target characteristics - not necessarily linked to a single offender	Statistical aggregation; hot spot identification; environmental factor analysis
Crime Trend	A statistically meaningful change in crime volume over time	Time series analysis; control charting; seasonal adjustment; communicating significance
Repeat Victimization	The same location, person, or target offended against multiple times	Address-level frequency analysis; flagging repeat victims for preventive intervention
Crime Spike	A short-term statistically anomalous increase in a specific offense type or area	Threshold-based alerting; root cause analysis; rapid product generation for operational response

Table 4.3: Crime pattern types and analyst responsibilities

4.4 Program Evaluation and Outcome Measurement

Crime analysts are responsible for evaluating whether departmental initiatives, enforcement strategies, and intervention programs are working. This requires understanding evaluation design, not just output measurement.

- Defining measurable outcomes before an initiative launches, not retrofitting metrics after the fact
- Establishing comparison baselines: prior-period comparison, comparison area methods, or matched control groups
- Accounting for displacement, whether crime reduction in a target area is accompanied by increases in adjacent areas
- Communicating the difference between correlation and causation when presenting program results to the command or city leadership
- Using regression-to-the-mean awareness: crime spikes often decline on their own; intervention timing should not be confused with intervention effect

DOMAIN 5 · Automation, Reporting & Visualization

Analytical output is only valuable when it reaches the right audience in a usable form, at the right time. This domain covers the tools and techniques analysts use to build repeatable reporting systems, automated workflows, and visualizations that make data accessible to operational and administrative users.

5.1 Business Intelligence and Dashboard Tools

Skill Area	Foundational	Proficient	Advanced
BI platform proficiency (Power BI, Tableau, ESRI Insights, etc.)	Navigates existing dashboards; modifies basic visuals	Builds dashboards from connected data sources; creates calculated measures	Designs enterprise BI solutions; manages data model and row-level security
Data modeling within BI tools	Uses pre-built data models	Creates relationships between tables; builds calculated columns and measures	Designs star/snowflake schemas optimized for analytical performance
DAX / calculated measures	Uses basic SUM, COUNT, AVERAGE measures	Writes time intelligence functions; context-aware measures	Builds complex measures with CALCULATE, FILTER, and advanced context transitions
Dashboard design principles	Applies basic formatting; chooses standard chart types	Designs for audience; applies visual hierarchy; minimizes cognitive load	Establishes agency dashboard standards; trains other staff
Refresh and scheduling	Understands manual vs. automatic refresh	Configures scheduled refresh; troubleshoots data source connectivity	Manages gateway configurations; builds monitoring for data pipeline health

Table 5.1: BI and dashboard tool proficiency matrix

5.2 Automation and Scripting

Automation is one of the most valuable time investments an analyst can make. Every repeatable manual task that is scripted and scheduled frees analyst time for higher-value analytical work and produces more consistent, timely outputs than manual processes allow.

Tool / Skill Area	Application in Crime Analysis
Python / R (scripting)	Data cleaning, scheduled reporting, statistical modeling, geospatial processing, API data pulls from external systems
Excel / VBA macros	Automating repetitive spreadsheet tasks; building structured report templates with calculated fields; legacy workflow automation
SQL scheduled jobs / stored procedures	Automating recurring data pulls; pre-aggregating summary tables; building alert logic that triggers on threshold breaches
Task Scheduler / cron jobs	Scheduling scripts and reports to run at defined intervals without analyst intervention
Power Automate/workflow tools	Triggering notifications, email alerts, and file movements based on data conditions; building approval and review workflows
ArcGIS Model Builder / Python (arcpy)	Automating multi-step spatial analysis workflows; batch geocoding; scheduled map production

Table 5.2: Automation tools and applications in crime analysis

5.3 Data Visualization Principles

Effective visualization is not decoration; it is the mechanism by which analytical findings reach decision-makers. Analysts must understand visualization best practices and the specific standards that apply to law enforcement audiences.

- Choosing chart types that match the data structure: bar charts for categorical comparisons, line charts for time series, scatter plots for correlation, maps for spatial distribution
- Avoiding visualization patterns that mislead: truncated axes, dual-axis abuse, overplotting, inappropriate use of 3D charts
- Designing for the operational context: shift briefings require different visualization standards than command presentations or city council reports
- Color choice for accessibility: avoiding red-green combinations that fail for color-blind readers; maintaining contrast ratios for projected displays
- Annotation and context: every analytical chart should include a title, source, time period, and any relevant caveats without a reader needing to ask

DOMAIN 6 · Professional Practice & Ethics

Technical competence alone does not define a professional crime analyst. The ethical obligations of the role to produce honest analysis, protect sensitive data, communicate uncertainty accurately, and maintain analytical independence are as fundamental as any SQL query or GIS technique.

6.1 Analytical Integrity

Analytical integrity is the commitment to producing analysis that is honest, reproducible, and independent of the outcome the requester prefers. It is the professional standard that distinguishes crime analysis from advocacy, and it must be maintained under pressure.

- Presenting findings accurately even when they are unfavorable to a preferred narrative, departmental initiative, or political position
- Distinguishing clearly between what the data shows and what conclusions might be drawn, and never conflating the two without explicit framing
- Documenting analytical methods so that findings can be reproduced, reviewed, and challenged
- Declining to produce an analysis that is designed to reach a predetermined conclusion, and escalating such requests appropriately
- Acknowledging the limitations of data and methods in every analytical product, not as a disclaimer, but as a professional obligation

THE INDEPENDENCE STANDARD

Crime analysts serve the data, not the requester. When command staff, supervisors, or political officials pressure analysts to change findings, reframe conclusions, or omit inconvenient data, the analyst's professional obligation is to resist that pressure and document the interaction. An analyst who produces whatever answer is requested is not performing analysis; they are producing a rationalization.

6.2 Data Privacy, Security, and Legal Compliance

Requirement	Analyst Responsibility
CJIS Security Policy[2]	Understanding and complying with FBI CJIS requirements for data access, storage, transmission, and disposal of criminal justice information
28 CFR Part 23[3] **(criminal intelligence)**	Understanding the regulatory framework for criminal intelligence systems; ensuring analytical products that reference intelligence sources comply with dissemination rules
PII handling and minimization	Limiting personal identifying information in analytical products to what is necessary; anonymizing or aggregating data appropriately for different audience tiers
Data sharing agreements	Understanding the legal basis and limitations of inter-agency data sharing; ensuring data received under MOUs is used only as authorized
Public records and FOIA	Understanding which analytical products and underlying data may be subject to public records requests; consulting legal counsel appropriately
Secure handling of sensitive data	Managing access controls, encryption, and secure transmission of sensitive law enforcement data; understanding the consequences of data breaches

Table 6.2: Legal and compliance requirements for crime analysts

6.3 Communication and Analytical Writing

Analytical findings have no operational value unless they reach the right audience in a form they can act on. Communication is a professional competency, not a soft skill.

- Writing analytical products that lead with findings, not methods: command staff need conclusions and recommendations, not methodology sections
- Calibrating product length and complexity to the audience: a shift briefing summary is not a research report

[2] Criminal Justice Information Services (CJIS) Security Policy, Version 6.0 (FBI CJIS Division, released December 27, 2024), available at le.fbi.gov/cjis-division/cjis-security-policy-resource-center
[3] 28 C.F.R. Part 23 — Criminal Intelligence Systems Operating Policies, available at ecfr.gov/current/title-28/chapter-I/part-23

- Using precise language: avoiding ambiguous terms like 'significant,' 'high,' or 'unusual' without a quantitative definition
- Producing verbal briefings that convey analytical findings clearly and answer follow-up questions without deferring to documents
- Writing for accountability: analytical products should be attributable, dated, and version-controlled

6.4 Professional Development and Continuing Education

The crime analysis profession evolves continuously. Tools change, methods improve, data systems are replaced, and the legal environment shifts. Analysts have a professional obligation to maintain current competency, and agencies have a reciprocal obligation to support that development.

- Maintaining awareness of developments in data tools, GIS platforms, and statistical methods, and AI-assisted analysis tools relevant to law enforcement contexts, including using them responsibly and verifying their outputs
- Pursuing NACA certification and continuing education requirements as a standard of professional practice
- Contributing to the profession through mentorship, peer review, training delivery, and knowledge sharing
- Engaging with published research on crime patterns, place-based policing, and evidence-based practices, and applying relevant findings to local contexts

Career Level Competency Summary

The following matrix summarizes expected proficiency levels by career stage across all six domains. This table is intended as a reference for hiring rubrics, performance review criteria, and career development planning.

Domain	Entry(0–2 yrs)	Mid(3–6 yrs)	Senior(7–12 yrs)	Lead / Mgr(10+ yrs)
1. Data Fundamentals & Literacy	Foundational	Proficient	Proficient	**Advanced**
2. Data Management & Infrastructure	Foundational	Proficient	Proficient	**Advanced**
3. Spatial Analysis & Mapping	Foundational	Proficient	**Advanced**	**Advanced**
4. Statistical Analysis & Pattern Recognition	Foundational	Proficient	**Advanced**	**Advanced**
5. Automation, Reporting & Visualization	Foundational	Proficient	Proficient	**Advanced**
6. Professional Practice & Ethics	Foundational	Proficient	**Advanced**	**Advanced**

Table: Career level competency expectations by domain

Using This Framework

For Hiring and Classification

Job postings for crime analyst positions should reference this framework explicitly, using domain language and proficiency levels to set honest expectations. Listing 'SQL,' 'GIS,' and 'data literacy' as requirements, with defined proficiency levels, is likely to produce better candidate pools and more defensible hiring decisions than generic requirements like 'analytical skills required.'

For Performance Review

Annual performance reviews for analysts should include a domain-by-domain self-assessment against this framework, with supervisor review. This creates a documented

developmental record and supports linking compensation decisions anchored to measurable professional growth.

For Compensation Advocacy[4]

When analysts or their advocates present compensation cases to HR departments or city councils, this framework provides the evidence base. Each domain contains skills that command significantly higher compensation in comparable private-sector roles. National survey data show crime analysts earning 10–30% below data analysts, research analysts, and federal intelligence analysts with similar credentials, and receiving smaller cumulative pay increases than sworn officers over time (2024 MARCAN Salary & Benefits Survey and the 2026 International Crime Analyst Census Survey, Central Washington University). This pattern has been documented for decades: a 2003 U.S. Department of Justice survey of crime analysis units found that civilian analysts performing work comparable to sworn personnel were paid substantially less, contributing to high turnover (O'Shea & Nicholls, 2003). The framework makes visible the breadth and depth of competency that agencies receive, often at below-market cost.

For Training Planning

NACA training programs, continuing education requirements, and certification pathways are aligned to this framework. Analysts and their supervisors can use domain proficiency gaps to identify targeted development investments.

For Assessing Current Standing

NACA has developed a Command Capacity Assessment as well as an Analyst Self Assessment. These structured assessments will aid in the evaluation of an agency's crime analysis capacity, infrastructure, investment, and operational integration.

National Association of Crime Analysts (NACA)
The Voice of Crime Analysis | naca-usa.org

[4] National Association of Crime Analysts. (2026). *Crime Analysis Salary & Compensation Report*, based on the 2024 Mid-America Regional Crime Analysis Network (MARCAN) Salary & Benefits Survey and the 2026 International Crime Analyst Census Survey (Central Washington University). Available at: O'Shea, T., & Nicholls, K. (2003). Police crime analysis: A survey of US police departments with 100 or more sworn personnel. *Police Practice and Research: An International Journal*, 4(3), 233–250.