

DCI Network: Agency New Technology Request Guide Submitting a Project Proposal and Implementation Plan

Introduction:

With on-going advancements in law enforcement technology, the North Carolina State Bureau of Investigation (SBI) remains committed in working with agencies to help implement creative solutions to meet their mission critical needs. NC SBI constantly evaluates and implements new technologies to help improve the service agencies receive and to keep fees reasonable.

DCIN is the North Carolina Criminal Justice System (CJIS) network used to exchange criminal justice/law enforcement information, which includes access to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) system network, more commonly known as NCIC (National Crime Information Center) and Nlets. Through provisions in the North Carolina Administrative Code (NCAC), the SBI also enforces state regulations regarding DCIN. In these roles, the SBI is responsible for administering access to NCIC/DCIN/Nlets, ensuring compliance with regulations and policies on appropriate use.

Different agencies have different needs. The SBI recognizes the advantages and options that new technologies can offer. The SBI will continue to remain in a position to support technology initiatives related to DCIN that can provide the tools for agencies to meet complex challenges in their jurisdictions.

To assist in exploring and implementing these new technologies, agencies should submit a Project Proposal and Implementation Plan to the SBI for prior review.

Project Proposal and Implementation Plan:

A formal implementation plan reduces project risk and enhances the potential for success of new technology initiatives. It helps to assure effective implementation and an understanding early of the policy and technical requirements for integration of new applications. Collaboration with key stakeholders and end users during the entire implementation process is critical to project success.

- Guidelines:*
1. Your agency should complete and submit a Project Proposal and Implementation Plan (see Components).
 2. Include a cover letter from your agency head, on agency letterhead.
 3. Attach the Project Proposal and Implementation Plan to the cover letter, along with any supporting documentation.
 4. See Contact Information for sending your request.
 - Working directly with agency representatives on initial project needs, and not vendors, is best practice. At later stages in the process, our IT staff will work with agency-selected vendors to implement solutions at the agency level.
 - The SBI does not endorse individual vendors, products or services and does not advise technology users that any one vendor is rated higher than another.
 - The SBI reviews agency proposals for policy and technical feasibility.
 - Some requests require FBI and Nlets reviews and approvals.

Project Proposal and Implementation Plan:

Components: Agencies should complete a detailed proposal and plan for each new technology initiative to include at a minimum the following:

1. Implementation Brief

- a. Give a project overview, including anticipated start/end dates.
- b. Identify people involved in the implementation.
 - i. Project team and team lead(s).
 - ii. Agency DCIN TAC/POC.
 - iii. Vendor liaison and contact information.
 - iv. Business process advisors.
 - v. Other stakeholders (e.g., end users, for usability planning during implementation, area law enforcement partners, courts).

2. Timeline

- a. List milestones, major dependencies, responsible party/parties for each milestone.
- b. Identify risks if timeline not met; include regulatory, compliance, legal and financial risks.

3. Communication Plan

- a. Outline how the project will be communicated.
- b. Identify communications internal to the project team (e.g., regular meeting dates), external to the project team (e.g., SBI), and with vendors.

4. Physical Plan

- a. Identify physical implementation requirements, to include new equipment/new use of existing equipment; network and telecommunications requirements and implications.
- b. Address physical security concerns.

5. Process Impact Plan

- a. Identify and address new process needs or requirements.
- b. Outline impact on agency, mission critical need, and overall operations.
- c. Identify and detail specific request(s) being made by the agency to the SBI.

6. Testing Plan

- a. What is to be tested?
- b. How will the test be conducted?
- c. Who is responsible for each testing item?
- d. Who will have a role in the testing?
- e. Who will review the test results (verify process for audit controls; assure reconciliation, data integrity, data transfer as planned)?

7. Training Plan

- a. If training or on-going performance support is required, outline the plan.
 - i. Describe initial training.
 - ii. Training aids (for use with minimal or no training).
 - iii. On-going performance support (to ensure backup and sustainability in case current system "experts" are not available).

-
- b. Provide copies of agency training materials for impacted stakeholders when submitting your proposal and plan.

**Project Proposal and
Implementation Plan:**

Components: **8. Review Controls**

- a. Have requirements for the following been met?:
 - i. Compliance, regulatory or legal requirements.
 - ii. Data security.
 - iii. Necessary backups.
 - iv. Data integrity assurance process in place and operational.
- b. Have requirements outlined in the FBI CJIS Security Policy, NCIC Manual, Nlets User and Technical Manual, North Carolina General Statutes (NCGS) and North Carolina Administrative Code (NCAC) that your proposal/plan impact been met?
- c. Does the vendor meet FBI CJIS certification and security addendum requirements?
- d. Has a state of residency and national fingerprint based background check been conducted on all vendor employees as part of a comprehensive background screening by the agency?
- e. Has a review been conducted for compatibility with existing technology systems or other systems?

9. Backups and Workarounds

- a. Identify backups and workarounds in place during implementation.
- b. List any continuity issues.

10. Transition to New Owners/Users

- a. Establish hand-off criteria and conditions.
- b. Identify timing, date/time and roles in transition to new owners/users.

11. Feedback

- a. Provide feedback processes before, during and after the implementation:
 - i. Output feedback.
 - ii. Input feedback.
 - iii. Milestones and adjustments
- b. Are outcomes meeting expectations (e.g., at each milestone and for project as a whole)?
- c. Include feedback in regular team communications.

Contact Information:

North Carolina State Bureau of Investigation
Criminal Information and Identification Section
3320 Garner Road
PO Box 29500
Raleigh, NC 27626-0500

Attn: Ivy McMillan, Special Agent in Charge
Criminal Information and Identification Section

Re: NCIC/DCIN/Nlets Systems Access
Agency New Technology Implementation

Authority:

- FBI CJIS Security Policy.
- NCIC Manual.
- Nlets User and Technical Manual.
- North Carolina General Statutes: 143B-902 Through 143B-905, 143B-906, 143B-915, 143B-917
- North Carolina Administrative Code: 14B NCAC 18A.0201, Eligibility for Full or Limited Access to the DCI Network; 14B NCAC 18B.0407, Research Use and Access of CCH Records.

Online Resources:

FBI CJIS Security Policy:

<https://le.fbi.gov/cjis-division-resources/cjis-security-policy-resource-center>

DCIN / Omnixx
Links, IT Assistance, CJIS Security Policy

North Carolina Administrative Code:

<http://reports.oah.state.nc.us/ncac.asp>

Title 14B Public Safety, Chapter 18 Division of Criminal Information

Questions:

Policy: TACHelp@ncsbi.gov

Technical: BISL@ncsbi.gov

Early in the process, your agency should contact our IT staff with any technical questions:

ServiceDesk@ncsbi.gov

(919) 773 - 7900