Integration capability matrix

NCCIA

Generated
2026-09-29 11:14:23

Important

No live integration is claimed in this document. A capability is marked verified live only after an authorised end-to-end exchange has been completed and recorded. Every other row states the exact approval, documentation, credential or network access still missing. Row-level technical notes are reproduced verbatim in English so they can be matched against the authority's own records.

1. Intended counterparty

Legal entity (intended target)
National Cyber Crime Investigation Agency (intended target)

Trading name
NCCIA

Category
Federal cybercrime investigation agency

Jurisdiction
Federal / cross-jurisdiction

Identity verified from
NOT VERIFIED against an official source

Verification date
—

Integration owner
None in place

Support route
None in place

Data-sharing agreement reference
None in place

System categories assessed
4

Verified live today
0

City / district endpoints
—

2. System categories and current standing

Cybercrime referral

Intended integration
Prepare a reviewed cybercrime referral to the agency's accepted procedure

Current state
Sandbox

Vendor
AETNIC simulator

Environment
Sandbox (simulator)

Documented interface version
sim-1.0

Authentication method
none (local simulator)

Permitted read operations
receiveStatusEvent

Permitted write operations
createOperationalTicket, getRequestStatus

Data-sharing agreement reference
None in place

Data classification
internal

Rate limits
none (local)

Health check
always healthy

Support owner
AETNIC delivery team

Last successful exchange

Never

Credential / certificate expiry
None in place

Acknowledgement capability
Supported in principle

Verification capability
Not established

Blocking dependency
SIMULATOR — not a live connection. Demonstrates the workflow only. To go live: Requires: (1) a signed data-sharing or interconnection agreement with National Cyber Crime Investigation Agency (intended target); (2) the vendor's the organisation's interface documentation and its version; (3) credentials or certificates issued to THIS application; (4) network access / allowlisting to the receiving endpoint. None of the four is in place.

Cybercrime referral

Intended integration
Prepare a reviewed cybercrime referral to the agency's accepted procedure

Current state
Manual submission

Vendor
Not asserted — verify with the authority

Environment
Production

Documented interface version
Not asserted — verify with the authority

Authentication method
Not asserted — verify with the authority

Permitted read operations
None in place

Permitted write operations
None in place

Data-sharing agreement reference
None in place

Data classification
restricted

Rate limits
Not asserted — verify with the authority

Health check
Not asserted — verify with the authority

Support owner
None in place

Last successful exchange
Never

Credential / certificate expiry
None in place

Acknowledgement capability
Supported in principle

Verification capability
Not established

Blocking dependency
Requires: (1) a signed data-sharing or interconnection agreement with National Cyber Crime Investigation Agency (intended target); (2) the vendor's cybercrime_referral interface documentation and its version; (3) credentials or certificates issued to THIS application; (4) network access / allowlisting to the receiving endpoint. None of the four is in place.

Evidence preservation request

Intended integration
Request preservation of source material with provenance intact

Current state
Manual submission

Vendor
Not asserted — verify with the authority

Environment
Production

Documented interface version
Not asserted — verify with the authority

Authentication method
Not asserted — verify with the authority

Permitted read operations

None in place

Permitted write operations
None in place

Data-sharing agreement reference
None in place

Data classification
restricted

Rate limits
Not asserted — verify with the authority

Health check
Not asserted — verify with the authority

Support owner
None in place

Last successful exchange
Never

Credential / certificate expiry
None in place

Acknowledgement capability
Supported in principle

Verification capability
Not established

Blocking dependency
Requires: (1) a signed data-sharing or interconnection agreement with National Cyber Crime Investigation Agency (intended target); (2) the vendor's evidence_preservation_request interface documentation and its version; (3) credentials or certificates issued to THIS application; (4) network access / allowlisting to the receiving endpoint. None of the four is in place.

Investigation correspondence

Intended integration
Register investigation-related correspondence and clarification

Current state
Manual submission

Vendor
Not asserted — verify with the authority

Environment
Production

Documented interface version
Not asserted — verify with the authority

Authentication method
Not asserted — verify with the authority

Permitted read operations
None in place

Permitted write operations
None in place

Data-sharing agreement reference
None in place

Data classification
restricted

Rate limits
Not asserted — verify with the authority

Health check
Not asserted — verify with the authority

Support owner
None in place

Last successful exchange
Never

Credential / certificate expiry
None in place

Acknowledgement capability
Supported in principle

Verification capability
Not established

Blocking dependency
Requires: (1) a signed data-sharing or interconnection agreement with National Cyber Crime Investigation Agency (intended target); (2) the vendor's investigation_correspondence interface documentation and its version; (3) credentials or certificates issued to THIS application; (4) network access / allowlisting to the receiving endpoint. None of the four is in place.

3. Prerequisites before activation

A signed data-sharing or interconnection agreement with the organisation named above.
The vendor's interface documentation, including its version, for each system category.
Credentials or client certificates issued to THIS application (not shared operator accounts).
Network access and allow-listing to the receiving endpoint, plus an agreed environment (sandbox first).
A named integration owner on both sides and an agreed support escalation route.
An agreed data classification and retention profile for each data type exchanged.
One successfully completed authorised end-to-end exchange in non-production before any production activation.

4. Limitations

This matrix describes INTENDED integration and current standing, not an achieved capability.
Where an identity has not been verified against an official source, it is marked NOT VERIFIED.
An entry in the directory does not imply that the organisation operates an accessible interface.
Connections marked sandbox are labelled simulators used to demonstrate workflow only.