Exception Information

Contents

Section 1: General Information

Submission

- Please ensure your agency is using and accessing the most current forms and links.
- Submit requests to dit.exceptions@nc.gov
- Please complete all fields. If a section does not apply, note N/A.
- Attach or reference all supporting documentation.
- Complete the Justification section supporting your exception (e.g., non-DIT hosting, reason for waiver of competition) and your Business Case which describes the business operations related to the exception.
- If your request has multiple exceptions (e.g., sole source waiver with third party vendor hosting), your agency must complete each form and submit as a complete package.
- Please help our agency in processing your request as quickly as possible by ensuring a complete submission.
- **Personal Services Contracts** pursuant NCGS § 143B-1362 are outside the scope of the exception process. Your agency should work directly with DIT Strategic Sourcing to discuss what options are available to your agency under current laws.

Questions

- Early engagement and partnership between business owners, IT, sourcing, and internal stakeholders, and DIT is key when defining your submission.
- Specific subject-matter questions, contact a respective DIT team member (project, security, sourcing, standards).
- General questions, email us at dit.exceptions@nc.gov

Section 2: Security

Information

- Submit Form C with supporting documents as attachments.
- Agencies should review and ensure that all required security policies are in place to protect sensitive data; refer to the Statewide Information Security Manual
- Pursuant to NCGS § 143B-1377, agencies must complete the necessary security, risk, and/or data classification assessment for each request. Agencies should use the Privacy Threshold Analysis form to assist with this effort.
- Your agency may have a procurement for a business solution that includes services handling sensitive or confidential data (e.g., PII, HIPAA, FERPA). Use the Privacy Threshold Analysis (PTA) form to assess the types of data and potential risks involved. PTAs are not required for Security Exceptions (Form C).
- The agency Chief Information Security Officer (CISO) or their designee should include a statement of review and/or compliance consistent with agency and state standards with each exception submitted.

- **Information Security Incidents** (e.g., intrusion, hacking, information disclosure, denial of service, exploitation, cyber-attack) are not exceptions and should be reported at: https://it.nc.gov/cybersecurity-situation-report

Privacy Threshold Analysis (PTA)

- The Privacy Threshold Analysis form is available to assist agencies in assessing system and application privacy implications.

Industry Certification Report

- In some cases, pursuant to NCGS § 143B-1378, agencies will need to provide an industry certification report and in particular, for cloud-based hosting or application solutions.

- Agencies will need to contact their vendor, obtain, and provide a copy of its most recent third party audit. Examples include SOC 2 Type 2, SSAE 18, ISO 27001, or FedRAMP certification reports.

Questions

- DIT Enterprise Security and Risk Management Office (ESRMO): security@its.nc.gov

Section 3: Sourcing

Information

- Submit Form A with supporting documents as attachments in editable formats.
- Include all procurement-related documents (e.g., contracts, amendments, Request for Quote/RFQ, Request for Proposal/RFP, Invitation for Bid/IFB, waiver justifications, costs, vendor quotes, Agency approvals).
- Ensure your agency has a valid, existing contract to extend/amend and that justifications meet procurement and legal thresholds.
- Work with your business owner to align your agency business needs with your procurement avenue.

Sourcing Packet

- A sourcing or procurement packet may include, but is not limited to, any of the following in editable formats:
  - Draft Solicitation (IFB, RFQ, RFP)
  - Vendor Quotes
  - Draft Amendment
  - Draft Notice of Extension

Competition

- Always seek full competition whenever competition is available. When full competition is not available, an exception may be submitted for limited or waived competition pursuant to 09 NCAC 06B.0901
- Each justification must explain why the product or service is singularly able to meet the requirements of the user and must conclusively support the determination that no other product or service can fulfill user needs.
- Agencies have authority to grant waivers of competition for procurements within their delegated authority level; follow normal procurement procedures.

Limited Competition

- May be used when more than one vendor can supply a particular brand of product or brand of service to meet agency requirement.

Waived Competition

- May be used when only one vendor can provide a particular product or service to meet agency requirement.
- The requirement can only be met by a unique good or service that is not offered by any other vendor; there is only one source of supply.

Contract Beyond 3 Years

- Do you have a request involving a contract longer than 3 years? If Yes, an exception must be submitted. If your answer is No, follow DIT Strategic Sourcing procedures; no exception is required.

Existing Built-In Optional Renewals

- If your agency has an approved, existing contract with existing built-in optional renewals, and that will carry your contract beyond 3 years, no exception is required.
- Your agency must still submit all required paperwork to DIT Strategic Sourcing in advance for each renewal option to be exercised.
- The last year of a renewal option will not be approved without the agency providing a plan of action for the following year.
- Only when all renewals are exhausted and your agency plans to continue with an agreement that would limit or waive competition, will an exception be required.

State Term Contracts

- If a State Term Contract exists to support your needs, usually no exception is required, unless purchasing equipment that will not be located at either the Eastern Data Center or Western Data Center.
- Review the list of available contracts and/or partner with the respective managing Strategic Contracting Officer for that contract with any questions.

Questions

- Contact your assigned agency Statewide IT Procurement Office Contracting Officer or Specialist.

Section 4: Standards

Information

- Submit Form B with any attachments.
- The State Chief Information Officer (SCIO) has statutory authority in planning and managing a framework that collaboratively develops and publishes, information technology standards that guide architecture, design, engineering, procurement, and operational activities.

Hosting

- NCGS § 143B-1365[1] requires State agencies to use the State infrastructure to host their projects, services, data, and applications pursuant to current guiding authorities/laws.
- Agencies seeking an exception must demonstrate justification in one of the following areas:

    1. Using an outside contractor would be more cost-effective for the State.
    2. The Department does not have the technical capabilities required to host the application.
    3. Valid security requirements preclude the use of the State infrastructure, and a vendor can provide a more secure environment.

[1] *NCGS § 143B-1365. Data Centers.*

(a) The State CIO shall create an inventory of data center operations in the executive branch and shall develop and implement a detailed, written plan for consolidation of agency data centers in the most efficient manner possible. By May 1, 2016, the State CIO shall present a report on the data center consolidation plan to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division. (b) State agencies shall use the State infrastructure to host their projects, services, data, and applications. The State Chief Information Officer may grant an exception if the State agency can demonstrate any of the following: (1) Using an outside contractor would be more cost-effective for the State. (2) The Department does not have the technical capabilities required to host the application. (3) Valid security requirements preclude the use of State infrastructure, and a vendor can provide a more secure environment. (2015-241, s. 7A.2(b).)

NCID

- The State Chief Information Officer (SCIO) strives to simplify electronic transactions with North Carolina State Government. The SCIO is required to ensure this happens in a secure manner. This is accomplished through authentication of users and controlled access to applications and services.

- To achieve this, the SCIO requires all inter-agency and external facing solutions/applications that create content use the State's Identity and Access Management solution ("NCID").

- More information on the NCID service can be found at: https://it.nc.gov/ncid/ and https://it.nc.gov/services/nc-identity-management-ncid

- NCID is used to integrate with numerous systems to synergize the end-user experience by providing authentication/authorization to State applications and solutions. All solutions requiring NCID authentication must externalize identity and access management and support the following protocols:

    - Security Assertion Markup Language (SAMLv2)
    - Lightweight Directory Access Protocol (LDAP)
    - Web Services (SOAP/WSDL)

- As existing solutions are upgraded or replaced, they will be required to support the above protocols.

- A formal exception is required to use a solution other than NCID. The agency must provide just cause for the exception to be approved.

Questions

Section 5: Writing Your Business Case

The following guidelines may be helpful to include when writing your business case.

1. Regulatory Authority:
   - Is there state, Federal, or other regulations driving your business need?
   - What alternatives were explored to attempt compliance?

2. Costs:
   - Attach list of services, equipment, or items to be purchased.

3. Risks:
   - Describe associate risks, risk that may be introduced, why the risk is tolerable.
   - Describe interfaces and technical environment that will exist with the exception.
   - How will risk management be evaluated?

4. Data Classification:
   - Use the Privacy Threshold Analysis form to describe the types of data (e.g., PII, HIPAA, FERPA) being managed, processed, how stored, or transmitted, directly and indirectly, involved and where hosted.

5. Impact:
   - What users and customers are impacted by this exception?
   - What are the implications if this exception is not approved?

6. Compensating Controls:
   - What controls will be put in place to mitigate risk to acceptable levels, when?
   - Identify security methodology to manage data and access to include logical security via application, system, database, or other means, as well as physical security of hardware and other related infrastructure.
   - Exceptions that create significant risks without compensating controls will not be approved or acknowledged without requiring further agency action.

7. Mitigation:
    - Mitigation must equal or exceed those of the exception.
    - Address both initial and ongoing implementation. Include information on hardware, software, infrastructure, training and procedural documentation, administrative and support personnel, consultants and vendors, disaster recovery, back-up, business continuity, and monitoring.

8. Exception Strategy:
    - Detail how the above controls will be maintained and reviewed by your agency.
    - List responsible parties for maintenance and review.
    - Outline the agency timeframe for coming into compliance.

9. Describe any additional information relevant to understanding this exception.

Section 6: References

Authority

- Assessment of Agency Compliance with Security Standards. NCGS § 143B-1378
- Cash Management for the State. NCGS § 147-86.11(f)(4)
- Conditions for Limited or Waived Competition. 09 NCAC 06B.0901
- Contract Beyond 3 Years. 09 NCAC 06B.0301
- Cooperative Purchasing. 09 NCAC 06B.1006
- Data Centers. NCGS § 143B-1365
- Exceptions. NCGS § 143B-1320(c)-(d)
- Personal Services Contracts. NCGS § 143B-1362
- Planning and Financing State Information Technology Resources. NCGS § 143B-1330
- Powers and Duties of the Department. NCGS § 143B-1321
- Procurement of Information Technology. NCGS § 143B-1350
- Project Management, Standards. NCGS § 143B-1340, 1341
- Security. NCGS § 143B-1375
- State CIO Approval of Security Standards and Risk Assessments. NCGS § 143B-1377
- State CIO Duties. NCGS § 143B-1322
- Statewide Information Security Manual
- Statewide IT Contracts
- Statewide Security Standards. NCGS § 143B-1376
- Transition to Department of Information Technology. NCGS § 143B-1325

Contacts

- Project Management Advisors (PMA)
- Strategic Sourcing Agency Team Assignments

Forms

- Exception Resources, Forms, and Information
- IT Procurement Forms and Templates
- Privacy Threshold Analysis Form