# **CCDC Inject Writing Guide**

*A structured approach to composing clear, effective, and high-scoring inject responses during competition.*

## **Purpose**

Injects are business-driven tasks assigned during the competition. Your goal is to demonstrate technical competence, professionalism, and your ability to align technical actions with business needs. This guide will help you write responses that are well-structured, concise, and aligned with what judges and white team evaluators expect.

## **Understanding the Inject**

Before taking any action, read the entire inject carefully and ask the following:

1. **What is being asked?** Identify the task, the deliverables, and any specific requirements or constraints.
2. **What type of inject is it?**
   * Technical (e.g., configure DNS logging, block a port, change passwords)
   * Policy or documentation (e.g., write an acceptable use policy)
   * Business or strategic (e.g., security posture report, proposed upgrades)
   * Communication (e.g., draft a message to staff or the public)
3. **What format is expected?**
   * Is a formal document required, or will a short memo suffice?
   * Are screenshots, logs, or configurations requested?
   * Is there a word limit, specific audience, or file format?
4. **Who should handle it?** Assign the task to a teammate with relevant knowledge and capacity. Avoid duplicate work by clearly marking ownership in your team’s tracking system.

## **Writing Framework**

Use the following structure when composing your response:

### **1. Executive Summary (1–2 sentences)**

Start with a high-level summary of your response. This should clearly state what was done or what is being proposed. Aim for clarity and brevity.

**Example:** We have enabled DNS query logging on DNS01. Logs are now being written to C:\DNSLogs, and a sample log entry is attached below.

### **2. Technical or Policy Detail (3–6 bullet points or short paragraphs)**

Explain the technical implementation, decision-making process, or policy content in concise and specific terms. Avoid unnecessary detail or filler language. Be factual, and use terminology appropriately.

**Example (Technical):**

* Enabled debug and analytical DNS logging via Event Viewer
* Configured log output to C:\DNSLogs\dnsdebug.etl
* Verified entries are appearing for all external query attempts
* Confirmed logging did not interfere with scoring checks
* Included screenshot showing configuration panel and log directory

**Example (Policy):**

* The policy outlines acceptable use for internal systems
* Users are prohibited from installing unauthorized software
* Passwords must meet minimum complexity and rotation standards
* Cloud storage and email services must follow company data guidelines
* Policy is based on NIST SP 800-53 and ISO/IEC 27001 recommendations

### **3. Recommendations or Next Steps (Optional)**

If applicable, include suggested future actions or operational considerations. Avoid adding speculative content unless it clearly adds value.

**Example:** To improve monitoring, we recommend forwarding DNS logs to a centralized SIEM, such as Splunk, if available.

## **Best Practices by Inject Type**

### **Technical Tasks**

* Include verification steps (e.g., screenshots, config paths, log entries)
* Be specific about what system was changed and how
* Consider whether your action could affect service availability or scoring

### **Policy or Documentation**

* Use professional tone and formatting
* Avoid jargon or overly technical language unless appropriate for the audience
* Reference real standards or guidelines when applicable

### **Communication Tasks**

* Match tone to the context (e.g., formal for external, direct for internal)
* Keep language clear, accurate, and non-alarmist
* Provide the facts; avoid speculation

## **Submission and Documentation**

* Submit injects through the official NISE portal or assigned platform
* Maintain a copy of your submission in your team’s shared folder
* Update your team tracker with:  
  + Inject title
  + Assigned owner
  + Submission timestamp
  + Associated system (if any)
  + Status (e.g., In progress, Submitted)

## **Pre-Submission Checklist**

Before submitting your response, review the following:

* Have I addressed every requirement from the inject?
* Is the writing clear, concise, and free of spelling/grammar issues?
* Have I included technical evidence or context if required?
* Is the tone appropriate for the intended audience?
* Would someone unfamiliar with the issue understand what was done and why?