



New York State Technology Enterprise Corporation

Report to New York State  
Board of Elections

For

NYSTEC Review of CIBER Security  
Master Test Plan V 5.0 and 5.1

Submitted to:

New York State Board of Elections  
40 Steuben Place, Albany NY 12207

October 27, 2006  
Version 1

This Page Intentionally Left Blank

## **Introduction:**

NYSTEC has been engaged by the SBOE to do an independent review of security test plans being developed by CIBER. On September 27, 2006, NYSTEC provided the NYS Board of Elections (NYSBOE) with an independent security-related review of CIBER's Security Master Test Plan version 3.1. Since that time additional discussions have been conducted between NYSTEC and CIBER to explain revisions that NYSTEC recommended to that version of the Security Master Test Plan. CIBER then created version 5.0 and 5.1 of the Security Master Test Plan which is the topic of this analysis.

## **Analysis:**

This current analysis is a review of the CIBER Security Master Test Plan version 5.0 and 5.1, which was expected to include all of the recommendations and findings from the NYSTEC review of the earlier version. CIBER's version 5.0 and 5.1 was also supposed to include suggestions made during the October 18 and 19 meetings between NYSTEC and CIBER.

The CIBER Security Test Plan version 5.0 and 5.1 should have incorporated the 200+ NYSTEC recommended additional state and federal testing requirements identified in the prior reviews; however, NYSTEC has not verified that all additional requirements were incorporated.

NYSTEC remains concerned over the lack of a security source-code test plan and methodology. NYSTEC expected that a high-level source code review test procedure and plan would be included in this version of the CIBER plan, but it was not. The version 5.0 and 5.1 plan *does* include source-code tests for specific requirements; however, testing methodologies, procedures, and a plan for how to identify malicious code and for how to evaluate the code against known electronic voting threats are *not* present.

The CIBER security master test plan remains basically a listing of testing requirements derived from state and federal documents. The plan *does* now include named test methods; however, details on how the test method will test for the requirement (the actual testing procedures) are not provided. This is acceptable, based on CIBER stating that testing procedures and details will be provided in the next phase. Additional NYSTEC findings are slated, according to CIBER, to be addressed in the forthcoming CIBER voting-machine-specific security testing plans.

NYSTEC and SBOE have the following expectations for the forthcoming machine-specific Security Master Test Plans:

The source-code test plan will describe the methodology and tools needed to test the source code against all relevant requirements and voting threats.

The source-code test plan will address testing to ensure that the source code is free of malicious code, programming errors, and any other code that impacts the machine's ability to perform as designed and according to documented specifications.

For each requirement and threat to be tested against, the following will be provided:

Detailed test setup procedures,

A description of the test method used,

A detailed test procedure that tests for the existence of a control, effectiveness of the control and ability for a control to be circumvented, and

A listing of all document dependencies and test prerequisites.  
The inclusion of a list of machine-dependent attacks, a list of the threats to the voting machines that they must guard against, and the testing procedures and analysis to demonstrate this.

The test plan will address spots where vendors have failed to provide source code — determining if the code components are provided by COTS products. This may be the case for vendor-developed software components for which source code is not provided. NYSTEC believes that the vendor’s definition of “COTS software” should be scrutinized to ensure that all software it uses to define ballots and to process votes is subject to a source-code review unless it is *truly* a COTS product.

The test plan will define and utilize the penetration test methods. NYSTEC believes that CIBER’s use of the penetration testing test method is well justified and that this method should be a significant component in the machine-specific test plans. NYSTEC requests that the penetration test method enable determining whether the security control can be circumvented. NYS BOE expects and requires that the efficacy of security controls be tested. It is not sufficient to merely verify that a security control is present. Whether the security control can be circumvented must be determined — that is true test of the security control’s efficacy.

NYSTEC has the following expectation for how the Master Test Plan and Security Master Test Plans will address security:

The final version of the CIBER Master Test Plan will distinguish security-related tests and provide links to the appropriate section of the CIBER Security Master Test Plan. The Security Master Test Plan should be a true subset of the CIBER Master Test Plan. All requirements in the Security Master Test Plan must also appear in the CIBER Master Test Plan.

The CIBER Master Test Plan will include all functional tests from the state and federal requirements. NYSTEC identified several missing tests in earlier analysis.

NYSTEC has the following specific comments on the version 5.0 and 5.1 Security Master Test Plans:

Several of the NIST-related security tests that NYSTEC had questioned appear to have been removed. NYSTEC questions the reasons why they were initially included and why it is appropriate that they are now removed.

CIBER has stated that all source-code review work will be done via a manual inspection, line by line, of the source code. NYSTEC is concerned with the effectiveness of a code-review process that does not utilize automated tools, or a lab environment, or plans to compile and run the source-code models and/or subsystems under test conditions.