NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

(U//FOUO) CLASSIFICATION GUIDE FOR
CRYPTANALYSIS, 2-12

Effective Date: 13 September 2005

CLASSIFIED BY: [REDACTED] Chief, CES
REASON FOR CLASSIFICATION: 1.4 (c)
DECLASSIFY ON: 20291123

ENDORSED BY: [REDACTED] Director of Policy

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: 20291123
<table>
<thead>
<tr>
<th>Description of Information</th>
<th>Classification/Markings</th>
<th>Reason</th>
<th>Declass</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (U) The fact that NSA/CSS exploits cryptographic information security devices and systems.</td>
<td>UNCLASSIFIED</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>2. (C) The fact that NSA/CSS works with Second Party partners on exploiting cryptographic information security devices and systems.</td>
<td>CONFIDENTIAL</td>
<td>1.4 (c)</td>
<td>20291123</td>
<td></td>
</tr>
<tr>
<td>3. (S) The fact that NSA/CSS works with unspecified Third Party partners on exploiting cryptographic information security devices and systems.</td>
<td>SECRET</td>
<td>1.4 (c)</td>
<td>20291123</td>
<td></td>
</tr>
<tr>
<td>4. (U) The fact that NSA/CSS exploits unintended cryptographic vulnerabilities in commercial or indigenous information security devices and systems, as long as neither the vulnerability nor the targeted device/system is identified.</td>
<td>UNCLASSIFIED</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>5. (TS/SI) The fact that NSA/CSS makes cryptographic modifications to commercial or indigenous cryptographic information security devices or systems in order to make them exploitable.</td>
<td>TOP SECRET//COMINT at a minimum</td>
<td>1.4 (c)</td>
<td>20291123</td>
<td>(U) Specifying the specific system is protected by an ECI.</td>
</tr>
<tr>
<td>6. (U) The fact that NSA/CSS has cryptanalytic techniques to exploit cryptographic components of commercial or indigenous information security devices or systems.</td>
<td>UNCLASSIFIED</td>
<td>N/A</td>
<td>N/A</td>
<td>(U) Additional details will raise the classification and may be protected by an ECI.</td>
</tr>
<tr>
<td>7. (C) The fact that NSA/CSS has the ability to recover cryptovariables used to exploit commercial or indigenous cryptographic information security devices or systems.</td>
<td>CONFIDENTIAL</td>
<td>1.4 (c)</td>
<td>20291123</td>
<td>(C) Details of CV recovery are protected by an ECI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(C) Specifying a specific system for which we can recovery CVs is protected by an ECI.</td>
</tr>
</tbody>
</table>
8. (U) The fact that NSA/CSS successfully exploits cryptographic components of commercial or indigenous cryptographic information security devices or systems without specifying the device or system.
   Classification/Markings: UNCLASSIFIED
   Reason: N/A
   Declass: N/A
   Remarks: (U) Additional details will require the classification and may be protected by an ECI.

9. (U//FOUO) The fact that NSA/CSS successfully exploits cryptographic components of commercial or indigenous cryptographic information security devices or systems when the device or system is specified.
   Classification/Markings: TOP SECRET//COMINT at a minimum
   Reason: 1.4 (c)
   Declass: 20291123
   Remarks: (U) Additional details may be protected by an ECI.

10. (TS) The fact that NSA/CSS obtains cryptographic details of commercial cryptographic information security systems through industry relationships.
    Classification/Markings: TOP SECRET at a minimum
    Reason: 1.4 (c)
    Declass: 20291123
    Remarks: (C) Identification of the system or company is protected as COMINT and ECI.

(U) DEFINITIONS:

(U//FOUO) Information security device or system: A device or system that provides any of the following services for communications or information systems: confidentiality, data integrity, authentication and authorization.

(U//FOUO) Cryptanalytic vulnerability: A flaw in the design, implementation or system integration of cryptography used in an information security device, or a flaw in the way that a cryptographic information security device is used.

(U//FOUO) Unintended cryptographic vulnerability: Security is less than advertised by the manufacturer.

(U//FOUO) Indigenous: Non-commercial cryptographic information security system or device developed by a SIGINT target.

(U//FOUO) If you have any questions about the content of this page, contact [redacted] DC32, [redacted]