Contractor Requirements Document
(Supplemented) Form

<table>
<thead>
<tr>
<th>Directive #: CRD M 205.1-8 (Supplemented Revision 0)</th>
<th>Title: Cyber Security Incident Management Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable Contractor(s): PHMC X RCC X OccMed X PRC X MSC X</td>
<td>Other: WRPS, ATL, Westech, BNI</td>
</tr>
</tbody>
</table>

Section A – Headquarters CRD:

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors whose contracts involve information systems that collect, process, store, display, create, disseminate, or transmit national security or unclassified DOE/Government information.

Regardless of the performer of the work, the contractor is responsible for implementing and complying with the requirements of this CRD and the applicable Senior DOE Management Program Cyber Security Plan (PCSP).

The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. Contractor managers or system owners may specify and implement additional requirements to address specific risks, vulnerabilities, or threats within its operating unit/systems.

Section B – General Clarifications:

For the applicable PCSP referenced in Section A (above) refer to the latest Supplemented Revision to CRD O 205.1A.

Section C – Specific Clarifications:

None

Section D – General Supplemental Requirements

None.

Section E - Specific Supplemental Requirements:

None