例：IIA（内部監査人協会：Institute of Internal Auditors）[1]は、CIAOと協力関係を結び、リスク管理に関するガイドを用意し、情報セキュリティにおける監査者の役割について対話を開始。

また、「国家情報システム保護計画」を作成し、情報セキュリティに関する教育や人材育成に努めようとしている。

●国家情報システム保護計画

下記に示すように「人材教育・資源」と「研究開発」の2つに大別される。

「人的教育・資源」

1.「連邦サイバーサービス」

- 2001年度：2,500ドルの予算
- 情報セキュリティに関する教育、トレーニングを行う。
- 人事管理庁（OPM）が中心に「情報技術卓越センター」、「サービス奨学金」、「高等・中等教育機関アウトリーチプログラム」、「連邦職員情報セキュリティ啓蒙プログラム」の4つを主に行う。

□ 「情報技術卓越センター（CITE）」プログラム
セキュリティに関する最先端の教育やトレーニングを連邦職員に行う。

□ 「サービス奨学金（SFS）」プログラム
情報セキュリティを専攻する大学3，4年生と大学院生に対して奨学金を与えるプログラム。

□ 「高等・中等教育機関アウトリーチプログラム」
中高生に対して、大学において情報セキュリティを専攻したくなるような、将来の連邦政府IT職員を目指したくなるような教育を行う。またコンピュータセキュリティについての個人の責任と倫理について教育を行うことを目指す。

---

[1] IIAは、70,000名の会員を有し、国際的な専門家によって構成される協会で、内部監査人やその組織に対して調査や教育、資格、標準化、その他の活動を提供するサービスを行っている。

□　「連邦職員情報セキュリティ啓蒙プログラム」
連邦政府職員にセキュリティについて教育し、責任ある行動をとるように促すのが目的。

2．サイバー市民パートナーシップ

- 司法省とITAAが共同して立ち上げたプログラム。
- 米国の情報インフラの保護に努める民間と政府間の共同イニシアティブ。
- 中核プログラム「サイバー市民啓蒙キャンペーン」：
9～12歳の児童を対象に、様々なメディアを通じて啓蒙を行う。
- 民間企業と連邦政府の間で人材交流。各セクターでどのようにインターネット上の犯罪に対処しているかを学び、それぞれのベストプラクティスについて理解を深める。

「研究開発」

「クリティカル・インフラストラクチャ保護R&D」、「情報インフラ保護研究所」、「専門家審査チーム」、「連邦進入防止ネットワーク」の4つからなる。

1．「クリティカル・インフラストラクチャ保護R&D」

- 「脅威・ボルネライリティ・リスク評価」、「システム保護」、「進入監視・応答」、「復旧・再構築」の4点に主眼を置いたR&D。
- 省庁横断型イニシアティブ。
- 予算：6億600万ドル（内訳は5億2,700万ドルがサイバーセキュリティR&D。残りが物理的セキュリティ保護のためのR&D）

2．「情報インフラ保護研究所（I3P）」

- 連邦政府間、民間企業間、また連邦政府と民間企業間でのギャップを埋めることを第一の役割とする。
- 2001年予算：5,000万ドル（大統領要求）

3．「専門家審査チーム（ERT）」

- セキュリティの専門家を集めて専門家審査チームを創設。
- 2001年度予算：500万ドル（大統領要求）
- 連邦政府の情報システムのボルネラビリティを発見・修正。セキュリティへの脅威に対処できるようなシステムを整える。

4．「連邦進入探知ネットワーク（FEDNet）」

- これまで連邦省庁内には、すでに独自のネットワーク防衛システムが導入されている。特に国防総省にはJTF-CNDという軍事関連システムを一括監視するシステムが存在しているが、省庁を横断するセキュリティは脆弱、各省長官の情報共有も進んでいない。
- FIDNetは、JTF-CNDに類似するものを、国防総省以外の省庁ネットワークに適用しようというもの。それにより、連邦省庁における攻撃、進入検知を自動化し、ひとまとめにしたい。少ない人材で、各省庁に平均的なセキュリティを提供することを目指す。
  R&D予算として1,000万ドル（大統領要求）。

3．米国におけるサイバー犯罪への取組における問題点

（1）組織体制における問題点

米国におけるサイバー犯罪への対応は国の機関が中心であり、国の機関でも特に組織上はFBIが主導しているNIPCが中心となっている。しかし、その体制構造は図2に示したように非常に複雑かつまとまりがない状態と言っても過言ではなく、各機関からもその組織体制の脆弱性、対応能力の欠如が指摘されている。

特に、NIPCは「いかなる機関がデータを共有していようと、すべての情報に対する権利を要求し、すべての情報を法執行力に分類して、殆どの諸機関自らが支援する業界と同情報を共有できない」ようにしたため、各政府機関で問題となり、NIPCは殆どの情報をすべての関連諸機関と共有できなくなる状況となっている。2000年2月の時点で36政府諸機関のうち6機関を除くすべての機関がNIPCに対する支援を中止した。シークレットサービス、CIA（中央情報局）、NSA、DIA（国防省国防情報局）は非公式な同盟を結び、NIPCを経由しないで情報交換を行っている。

（2）官民協力における問題点

民間企業においては、情報自由法（FOLA）に起因する情報のプライバシーの保護が最大の問題となっている。官民協力による情報共有機関はInfraGard、NSTACなど各種あるが、外部への漏洩という潜在的な懸念を常に抱えている。

情報自由法（FOIA）： 政府に保管されている殆どの情報について、市民の要求に応じて公開することを義務付けるもの。機密情報、軍事情報、個人情報、FBIの事件ファイルなどの例外はある。企業が政府と共有した情報については、法的に非公開とすることは出来ない。