



*“We Help
Put America
Through
School”*

COD Encryption

November 15, 2001



Discussion Agenda

Risk Assessment

Regulations

Encryption Options

Cost Comparison

Recommendation

Implementation



Risk Assessment

- Risks
 - Privacy act data from CPS, LO Web, DLSS, FMS, and NSLDS is not encrypted when sent from the VDC to TSYS
 - HTTP data is protected via SSL encryption, but interface data is not encrypted between the VDC and remote locations
- Vulnerabilities
 - TSYS, CSC, or Sprint employees with physical access to the HW
 - Hackers hacking into network devices
 - An example site is: <http://www.phrack.org/show.php?p=44&a=19>
- Consequences:
 - Potential fines for SFA
 - Compromised public trust because of publicity



Government Regulations

▪ Privacy Act

- Agencies must: "...establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."
- "(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of--
 - (A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and
 - (B) the costs of the action together with reasonable attorney fees as determined by the court."

▪ SFA Extranet Policy

- Security policy: Confidential information should be protected when communicated over open networks.
- If the SFA extranet will allow viewing and/or transfer of confidential information (business units to decide on confidentiality of all but Privacy Act data), then some sort of protection is required.



Encryption Options

Router Encryption:

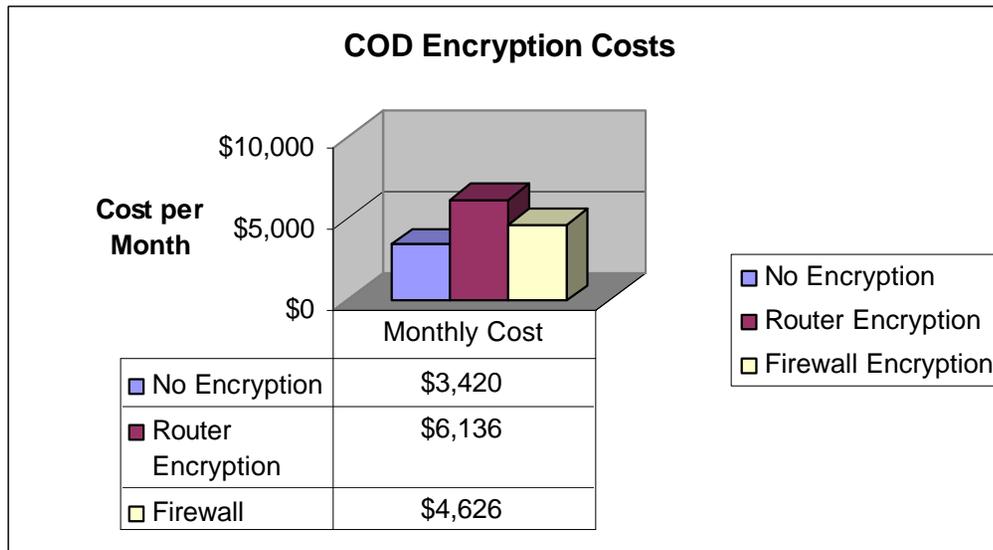
- Router Upgrade at the VDC
 - Upgrade required to support encryption
 - DES3 encryption
- Advantages
 - Better enterprise solution
 - Give all applications the ability to encrypt
 - Less HW at remote locations
- Disadvantages
 - More expensive
 - With move to house applications in the VDC, may be unnecessary

Firewall Encryption:

- Firewall encryption
 - Install a firewall at each remote location to encrypt between the remote location and VDC
 - DES3 encryption
 - Cost break even point for the two options is roughly 6 to 8 remote locations
- Advantages
 - Lower cost for COD
 - Only affects locations requiring encryption
- Disadvantages
 - More HW at remote locations
 - Less scalable at VDC



Cost Comparison Summary



- Base cost = \$3420 / mo. VDC charge for no encryption
- Firewall based option is \$3626 / mo., a \$1206 / mo. increase over no encryption
- Router based option is \$6136 / mo., a \$2716 / mo. increase over no encryption



Cost Comparison

- Base COD Network Costs
 - Base remote location VDC cost for COD is \$3420 / month
 - Only one COD connection would require encryption - VDC to TSYS
 - All the others are web traffic and secured using SSL
- Option 1 Costs:
 - \$6136 / mo. per remote location
 - \$73,632 annual cost
 - Cost difference from base cost is \$2716 / mo., \$32,592 per year
- Option 2 Costs:
 - \$4626 / mo. per remote location
 - \$55,512 annual cost
 - Cost difference from base cost is \$1206 per mo., \$14,472 per year
 - Cost savings of \$18,120/yr. over Option 1



Recommendation

- Our recommendation is to encrypt traffic between the VDC and TSYS utilizing an Enterprise Level encryption strategy (Option 1: Router Encryption).
 - Both options are technically acceptable from a data encryption standpoint and both provide the same level of encryption support. Option 2 is the most cost effective solution for COD.
 - Encryption of the link will provide “appropriate safeguards” for privacy act data.
 - Due to the slight incremental cost delta between the two options (\$18k annually), we recommend the long-term enterprise level option.