(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (PID)
Sent: Monday, September 26, 2011 1:48 PM
To: (b)(6), (b)(7)c (PID)
Subject: FW: Modification 1
Attachments: DOC.PDF

From (b)(6), (b)(7)c (PID)
Sent: Friday, September 23, 2011 11:04 AM
To: (b)(6), (b)(7)c (PID)
Subject: FW: Modification 1

FYI,

V

From: (b)(6), (b)(7)c (PRO)
Sent: Friday, September 23, 2011 9:57 AM
To: (b)(6), (b)(7)c (PID); (b)(6), (b)(7)c (PID)
Cc: (b)(6), (b)(7)c (PID)
Subject: Modification 1

Good morning,

Attached is the modification for Task Order HSSS01-10-F-0262, Cyveillance.

(b)(6), (b)(7)c
Small Business Specialist
202- (b)(6), (b)(7)c

From: (b)(6), (b)(7)c (PRO)
Sent: Thursday, September 22, 2011 9:47 AM
To: (b)(6), (b)(7)c
Subject: Modification 1

Good morning,

Modification for Task Order HSSS01-10-F-0262 is attached. The amount is $30,000.00. Please sign and return one copy of the modification.

(b)(6), (b)(7)c
Small Business Specialist
202- (b)(6), (b)(7)c

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Friday, September 23, 2011 3:00 PM
To: (b)(6), (b)(7)c (PRO)
Subject: RE: Modification 1
Attachments: USSS Mod 01 QinetiQ (092311).pdf

(b)(6), (b)(7)c

Attached hereto is the executed modification. Thank you for the modification.

Best Regards,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Thu 9/22/2011 9:46 AM
To: (b)(6), (b)(7)c
Subject: Modification 1

Good morning,

Modification for Task Order HSSS01-10-F-0262 is attached. The amount is $30,000.00. Please sign and return one copy of the modification.

(b)(6), (b)(7)c
Small Business Specialist
202- (b)(6), (b)(7)c

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (PID)
Sent: Wednesday, January 12, 2011 9:48 AM
To: (b)(7)c, (b)(6) (PID)
Subject: FW: Cyveillance
Attachments: Award.pdf; SOW_Cyveillance.doc

(b)(6), (b)(7)c

The only number I have is the contract # listed at the top of the Award document. Is this the same number that is used in the system?

(b)(6), (b)(7)c

(b)(6), (b)(7)c
Supervisory Protective Intelligence Research Specialist
U.S. Secret Service
Protective Intelligence and Assessment Division
Risk Management Branch
202 (b)(6), (b)(7)c direct)

From: (b)(6), (b)(7)c (PID)
Sent: Wednesday, October 27, 2010 4:57 PM
To: (b)(6), (b)(7)c
Subject: FW: Cyveillance

(b)(6), (b)(7)c
Senior Intelligence Advisor
UNITED STATES SECRET SERVICE
Protective Intelligence & Assessment Division
(o)
(c) (b)(6), (b)(7)c

From: (b)(6), (b)(7)c (PID)
Sent: Monday, October 18, 2010 10:11 AM
To: (b)(6), (b)(7)c
Cc: (b)(6), (b)(7)c
Subject: RE: Cyveillance

All,

Our conference call with Cyveillance is scheduled for 1pm this afternoon. Dial in instructions are provided below. This will be a technical requirements call, primarily between (b)(6), (b)(7)c and Cyveillance technical personnel.

Also, please find attached the Cyveillance contract. FYI, section 3.0 of the Statement of Work indicates the government is responsible for providing (b)(7)e

Thanks,

(b)(6), (b)(7)c
Special Agent

USSS-000111

U.S. Secret Service
Protective Intelligence and Assessment Division
Internet Threat Desk
Washington, DC
(b)(6), (b)(7)c Desk
Blackberry

From: (b)(6), (b)(7)c (PID)
Sent: Thursday, October 14, 2010 1:16 PM
To:
Cc: (b)(6), (b)(7)c
Subject: Cyveillance

(b)(6), (b)(7)c

Per our conversation earlier, here are the needs we have regarding the initial set up of the Cyveillance (b)(7)e

(b)(7)e

3. Cyveillance has requested a conference call between technical personal from Cyveillance and USSS to discuss requirements. Please let me know when you would be
available on Monday, October 18th, 2010 to participate in a call. The conference bridge is as follows:

Dial (b)(7)e. When prompted, enter the following number. (b)(7)e

Please let me know if you have any questions.

Thanks,

(b)(6), (b)(7)c
Special Agent
U.S. Secret Service
Protective Intelligence and Assessment Division
Internet Threat Desk
Washington, DC
(b)(6), (b)(7)c Desk
Blackberry

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (PID)
Sent: Friday, October 21, 2011 11:57 AM
To: (b)(6), (b)(7)c (PID)
Subject: Update from (b)(6), (b)(7)c

Hi (b)(7)c, (b)(6)

I will follow-up with (b)(6), (b)(7)c later, but this was his immediate response.

Hope this helps!

(b)(6), (b)(7)c

(b)(6), (b)(7)c
Supervisory Protective Intelligence Research Specialist
U.S. Secret Service
Protective Intelligence and Assessment Division
Risk Management Branch / Internet Threat Unit
(b)(6), (b)(7)c (direct)

From: (b)(6), (b)(7)c
Sent: Friday, October 21, 2011 11:49 AM
To: (b)(6), (b)(7)c (PID)
Subject: RE: Please give me a call

Good Morning (b)(6), (b)(7)c
I'm on conference calls for the next couple of hours but I will call you as soon as I'm finished. With respect to your questions:

1) The data deletion process has been completed and has passed through QA. We are in the process of implementing it (b)(7)e and it should be fully active by Monday. (b)(7)e as of today as well. I will send out a follow-up email on Monday just to give final confirmation that the task is completed.
2) I have referred your question to our (b)(6), (b)(7)c and he is working to get you an answer. I hope to have a definitive response shortly.

Please let me know if you have any additional questions or concerns and I will give you a call later on this afternoon to follow-up directly.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c
(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
2677 Prosperity Avenue Fairfax, VA 22031

(b)(6), (b)(7)c
Main: 1.888.243.0097
www.cyveillance.com

USSS-000152

From: (b)(6), (b)(7)c
Sent: Friday, October 21, 2011 11:44 AM
To: (b)(6), (b)(7)c
Subject: Please give me a call

Hi (b)(6), (b)(7)c

Are you available to give me a call today? My supervisor is trying to respond to our privacy officer on two things:

(1) Status of data deletion project (this is answer we need the most today) and implementation date.

(2) Response to the PIA question

Thanks
(b)(6), (b)(7)c

(b)(6), (b)(7)c
Supervisory Protective Intelligence Research Specialist
U.S. Secret Service
Protective Intelligence and Assessment Division
Risk Management Branch / Internet Threat Unit
(b)(6), (b)(7)c (direct)

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Tuesday, October 05, 2010 4:32 PM
To: (b)(6), (b)(7)c (CID)
Subject: Kickoff Presentation
Attachments: USSS Cyveillance Solutions Kickoff 10-10.pdf

Good afternoon (b)(6), (b)(7)c
Thanks for your time today and for making sure everything was coordinated. It was a pleasure meeting with you and your team and we look forward to working with you. Per our discussion attached is the kickoff presentation that we walked through today. I will follow up with you tomorrow with regards to the questionnaire and data exchange.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c

(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406

(b)(6), (b)(7)c

Main: 1.888.243.0097
www.cyveillance.com

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Wednesday, October 06, 2010 4:21 PM
To: (b)(6), (b)(7)c (CID)
Subject: Cyveillance Questionnaire and Information Exchange Forms
Attachments: USSS Information Protection Information Exchange Form 10-10.xls; USSS Corporate Security Information Exchange Form 10-10.xls; USSS Brand Intelligence Information Exchange Form 10-10.xls; USSS - Kick-Off Questionnaire 10-10.doc

Good Afternoon (b)(6), (b)(7)c
Per our discussion attached please find the Cyvelllance Questionnaire documentation and Information Exchange form for your services. The questionnaire documentation should give you an idea of the types of information that we're looking for while the information exchange docs are meant for you (b)(7)c I split them into three spreadsheets so each division would be able to populate their own.

Please feel free to expand, modify the information exchange doc as needed. In addition please let me know if you would like to schedule a follow-up meeting to discuss they types of information we are looking for.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c
(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406
(b)(6), (b)(7)c
Main: 1.888.243.0097
www.cyveillance.com

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Wednesday, October 13, 2010 3:22 PM
To: (b)(6), (b)(7)c (CID)
Cc: (PID)
Subject: RE: Contractor Forms
Attachments: (b)(6), (b)(7)c

Good Afternoon (b)(6), (b)(7)c -
Per your request please see the attached documentation. With respect to the technical meeting I will get some potential times for the meeting from my team and send them to you shortly. With respect to the CID configuration, I think tha(b)(7)e is fine. I think it would be helpful for them to provide us with their configuration requests (b)(7)e

Thanks and please let me know if you have any questions or concerns.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c

(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406

(b)(6), (b)(7)c

Main: 1.888.243.0097
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Wednesday, October 13, 2010 1:54 PM
To: (b)(6), (b)(7)c
Cc: (b)(6), (b)(7)c (PID)
Subject: RE: Contractor Forms

(b)(6), (b)(7)c

(b)(7)c, (b)(6) from our Protective Intelligence Division (PID), who you met at the kickoff, is cc'd on this email and should be kept in the loop on all correspondence. He will serve as the main facilitator for technical/infrastructure support during the build out to operations. Please advise when you have your technical folks ready to talk to(b)(6), (b)(7) guys so we can get the infrastructure in place as needed.

Please send the scanned copies through to both of us via email when ready. Since (b)(7)e will be working in the PID area while supporting numerous sections of this agency, (b)(6), (b)(7) will be the POC who will submit them to building management for access clearance. (b)(6), (b)(7)c please send (b)(6), (b)(7)c the correct mailing info so you can get hard copy also.

I'll be speaking with GPA later today to move them along in their answers. Also – while reviewing the first round questionnaires, I realized that any requests (b)(7)e by the Criminal Investigative Division (CID) (b)(7)e Because of this, I'm not sure that the questionnaires are needed for CID. Thoughts?

(b)(6), (b)(7)c
Assistant Special Agent in Charge
Criminal Investigative Division
US Secret Service
(b)(6), (b)(7)c (off)
(cell)

From: (b)(6), (b)(7)c
Sent: Tuesday, October 12, 2010 5:13 PM
To: (b)(6), (b)(7)c (CID)
Subject: Contractor Forms

Good Evening (b)(6), (b)(7)c
My apologies for the delay, we will have these two you prior to COB tomorrow. I will send scanned electronic copies and can send you hard copies as well. Is there a fax number or other desired method of transmission for the hard copies? Please let me know at your earliest convenience. Thanks in advance.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c
Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406
(b)(6), (b)(7)c
Main: 1.888.243.0097
www.cyveillance.com

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Thursday, September 30, 2010 10:09 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Prior to meeting on Tues.

Excellent, thanks (b)(6), (b)(7)c

Also can you add the following individuals to our attendee list?

(b)(6), (b)(7)c – Senior Solutions Sales Executive
(b)(6), (b)(7)c Solutions Assurance

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c
Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406
(b)(6), (b)(7)c
Main: 1.888.243.0097
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Wednesday, September 29, 2010 9:41 PM
To: (b)(6), (b)(7)c
Subject: Re: Prior to meeting on Tues.

If you bring a Thumbdrive with your presentation, we'll be good to go.

From: (b)(6), (b)(7)c
To: (b)(6), (b)(7)c (CID)
Sent: Wed Sep 29 17:01:17 2010
Subject: RE: Prior to meeting on Tues.

Hello (b)(6), (b)(7)c
I have listed the attendees below:

(b)(6), (b)(7)c Cyber Intelligence Division
(b)(6), (b)(7)c – Technical Manager
(b)(6), (b)(7)c Cyber Intelligence Division
(b)(6), (b)(7)c Threat and Fraud Analyst, Cyber Intelligence Division

With regards to the meeting itself, we will definitely have slides discussing background, methodology and capabilities. We will also be happy to go into greater detail and/or address any questions that your team has on the fly. Can you please confirm whether or not you will have a projector and a computer for us to use? If not we can prepare hard copy documents if necessary. Thanks for your help.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c

(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406

(b)(6), (b)(7)c

Main: 1.888.243.0097
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Wednesday, September 29, 2010 2:17 PM
To: (b)(6), (b)(7)c
Subject: Prior to meeting on Tues.

I'll need the names and titles of all attendees from Cyveillance for access purposes. Because of the number of personnel that are interested in the project here, I had to move the kick off to the Director's Conference Center. Is it possible for you to provide a brief presentation to the group which details Cyveillance's approach, systems and capabilities as well as the benchmarks and process of building the project out?

I'm out tomorrow and Friday. Hit me on the cell or via email if necessary.

(b)(6), (b)(7)c
Assistant Special Agent in Charge
Criminal Investigative Division
US Secret Service
(b)(6), (b)(7)c (off)
(cell)

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (PID)
Sent: Tuesday, January 03, 2012 5:44 PM
To: (b)(6), (b)(7)c
Cc:
Subject: FW: USSS: Cyveillance Employees w/ Building Access

Importance: High

Hi (b)(6), (b)(7)c

Per my conversations with (b)(6), (b)(7)c below is the complete list of Cyveillance personnel who hold/require USSS HQ badges. Please provide us with the list of expiration dates for the each of the below personnel and we work with the contractors to make sure we get their paperwork to you in a timely manner.

Also, (b)(6), (b)(7)c badge is currently expired. Does he need to complete his paperwork here at HQ, or can project manager (b)(6), (b)(7)c witness his documents if they completed and faxed back to HQ/ITU.

Thanks,
(b)(6), (b)(7)c

(b)(6), (b)(7)c
Supervisory Protective Intelligence Research Specialist
U.S. Secret Service
Protective Intelligence and Assessment Division
Risk Management Branch / Internet Threat Unit
(b)(6), (b)(7)c (direct)

From: (b)(6), (b)(7)c
Sent: Tuesday, January 03, 2012 5:16 PM
To: (b)(6), (b)(7)c
Cc:
Subject: USSS: Cyveillance Employees w/ Building Access
Importance: High

(b)(6), (b)(7)c

Per your request, here is a full list of all Cyveillance employees who have been granted building access.

(b)(6), (b)(7)c

Kind regards,
(b)(6), (b)(7)c

****

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Tuesday, June 22, 2010 11:01 AM
To: (b)(6), (b)(7)c (CID)
Cc: (CID)
Subject: RE: Contact

Thanks (b)(6), (b)(7)c

No real assistance needed as long as the bid is forthcoming soon.

The pressure on my side has just been mounting, particularly because of the requirement for (b)(7)e This could be a real challenge without some sense of time frame as I'm sure you can imagine.

Also, I got an email from (b)(6), (b)(7)c in procurement yesterday stating that the requirements for the RFP were still being defined, which raised concerns.

Is there any information you can share as to why you believe the bid will be out very shortly and how soon that will be? If you would rather talk by phone please give me a call. I tried your line a few minutes ago and chose to email rather than leave a message.

Thanks,
(b)(6), (b)(7)c

Best Regards,
(b)(6), (b)(7)c Business Development
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
(b)(6), (b)(7)c
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Tuesday, June 22, 2010 10:41 AM
To:
Cc: (b)(6), (b)(7)c (CID)
Subject: Contact

(b)(6), (b)(7)c

AD Rick Elias told me you had reached out for him the other day. He asked me to call you back and see if I can be of assistance as he is currently operationally tied up. If there is any information I can provide or questions you need answered, please let me know. On a possibly related note, believe it or not the bid process should be happening very shortly and we can hopefully move this operation forward.

Hope all is well. Please call with any questions.

(b)(6), (b)(7)c
Assistant Special Agent in Charge
Criminal Investigative Division
US Secret Service
(b)(6), (b)(7)c (off)
(cell)

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Tuesday, October 19, 2010 3:41 PM
To: (b)(6), (b)(7)c (CID)
Subject: Cyveillance Solutions Implementation

Hello (b)(6), (b)(7)c
I hope all is well. I was wondering if you had a quick minute to speak with (b)(6), (b)(7) and myself about the project. We just received notice that (b)(7)e and we just wanted to confirm. I had been working with (b)(6), (b)(7) to straighten out the logistics for the project and want to notify him that he doesn't need to proceed with that if this is in fact the case. Please let me know at your earliest convenience and we will jump on a quick conference call.

Thanks in advance.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c

(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406

(b)(6), (b)(7)c

Main: 1.888.243.0097
www.cyveillance.com

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (CID)
Sent: Monday, February 08, 2010 2:20 PM
To: (b)(6), (b)(7)c (CID)
Subject: FW: Cyber Safety 101 course

I ask for information and they will try to get something to me by Friday

---

From: (b)(6), (b)(7)c
Sent: Monday, February 08, 2010 1:26 PM
To: (b)(6), (b)(7)c (CID)
Subject: Re: Cyber Safety 101 course

Please call (b)(7)e passcode (b)(7)e since the three of us are in separate locations. Talk to you then.

From: (b)(6), (b)(7)c (CID)
To: (b)(6), (b)(7)c
Sent: Mon Feb 08 13:05:26 2010
Subject: RE: Cyber Safety 101 course
2 sounds good, should I call you or you call me

From: (b)(6), (b)(7)c
Sent: Monday, February 08, 2010 12:48 PM
To: (b)(6), (b)(7)c (CID)
Subject: Re: Cyber Safety 101 course

Hi (b)(6), (b)(7)c

Are you available today and if so, can you join (b)(6), (b)(7)c and I on a call at 2pm? I know the govt is closed today so tomorrow is fine but thought I'd check.

Thanks,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c (CID)
To: (b)(6), (b)(7)c
Sent: Fri Feb 05 12:04:10 2010
Subject: RE: Cyber Safety 101 course
Either...I will be here late today...I am not afraid of the "white-stuff"

From: (b)(6), (b)(7)c
Sent: Friday, February 05, 2010 12:01 PM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Cyber Safety 101 course

That might be our best bet as everyone seems to be heading out to beat the weather. If she gets back to me today and wants to talk should I try to reach you or would you rather plan for early next week?

From: (b)(6), (b)(7)c
Sent: Friday, February 05, 2010 11:52 AM
To: (b)(6), (b)(7)c
Subject: RE: Cyber Safety 101 course

No worries, we could do it next week if needed

From: (b)(6), (b)(7)c
Sent: Friday, February 05, 2010 11:19 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Cyber Safety 101 course

I am hoping this afternoon. I haven't heard from (b)(6), (b)(7)c yet today but she responded to me last night and said we could discuss your project today so I anticipate a call or message from her soon. She is working from home because of the storm so have to wait until I hear from her.

From: (b)(6), (b)(7)c
Sent: Friday, February 05, 2010 11:08 AM
To: (b)(6), (b)(7)c
Subject: RE: Cyber Safety 101 course

Yes....when could we all talk....

From: (b)(6), (b)(7)c
Sent: Friday, February 05, 2010 11:00 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Cyber Safety 101 course

Hi (b)(6), (b)(7)c

As you know, the internet is constantly evolving, so we have to do the same. (b)(4)

(b)(4)

Regarding pricing, I really think we should have another conversation with (b)(6), (b)(7)c to get a better sense of your specific goals for the solution, and then let her recommend a scope of work to meet those goals, for which we can then quote a price. Secret Service is a unique entity, and I don't think proposing (b)(7)e is necessarily the best route to take.

Does this make sense?

From: (b)(6), (b)(7)c
Sent: Friday, February 05, 2010 10:28 AM
To: (b)(6), (b)(7)c
Subject: RE: Cyber Safety 101 course

From a sales side.....could I get a price quote for (b)(7)e Does the price go down if the (b)(7)e is for three years?

From: (b)(6), (b)(7)c
Sent: Friday, February 05, 2010 9:43 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Cyber Safety 101 course

Hi (b)(6), (b)(7)c

Understood. These questions are best answered by (b)(6), (b)(7)c since she runs the group that you will be working with to implement. I forwarded your email to her last evening and she said she would answer today. I also forwarded your note below so she is on the same page. I anticipate a response today.

Thanks.
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Friday, February 05, 2010 9:40 AM
To: (b)(6), (b)(7)c
Subject: RE: Cyber Safety 101 course

(b)(6), (b)(7)c

I want to follow-up with some more details regarding the below requests....I am not looking for something with pretty pictures, it could be on a napkin, what we are trying to do is move beyond the ppt and the speeches and begin to roll-up our sleeves to get our arms around how this is going to fit into the organization, how the business/operations will engage this element, how information is going to flow.....you mentioned when an engagement begins, a questioner is provided to start the ball moving forward, I would like to get a copy of one and any other details/documents that might assist us get an idea of how cyveillance is going to get integrated into the way we conduct business.

Call me is you have additional questions
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c (CID)
Sent: Thursday, February 04, 2010 7:15 PM
To: (b)(6), (b)(7)c
Subject: RE: Cyber Safety 101 course

We had a good discussion today regarding this project....I am looking for some input/comments form cyveillance.

1. Could you provide a business flow (pictorial) of how information is exchanged between cyveillance and a customer. How is information requested, received, acquired, filtered, passed...
2. If we were to begin an engagement with cyveillance, how would you foresee the buildup of capability be accomplished. An outline or time line would assist in explaining your plan.

Thanks
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c (CID)
Sent: Friday, January 15, 2010 11:30 AM
To: (b)(6), (b)(7)c
Subject: RE: Cyber Safety 101 course

(b)(6), (b)(7)c

It was a pleasure meeting you in person at the presentation, thanks for taking the time (b)(6), (b)(7)c and I are working through this issue and hope to move the ball down the field shortly. As far as the training, I appreciate the offer but can't work it out.
Thanks again, I'm sure we'll be speaking live voice again soon.

(b)(6), (b)(7)c
Assistant Special Agent in Charge
Criminal Investigative Division
US Secret Service
(b)(6), (b)(7)c (off)
(cell)

From: (b)(6), (b)(7)c
Sent: Friday, January 15, 2010 11:19 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Cyber Safety 101 course

Hi (b)(6), (b)(7)c

I just got approval to comp this course for you (or someone else with your team), if you are interested, so you can evaluate it and see if its' something others at the agency should attend.

Please let me know. It's only a 4 hours course so not a huge time commitment and some great info.

Thanks,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Thursday, January 14, 2010 3:24 PM
To: (b)(6), (b)(7)c
Subject: Cyber Safety 101 course

Hello (b)(6), (b)(7)c

Thanks again for your time on Monday. As I'm sure you are aware, I've been corresponding with (b)(6), (b)(7)c since and we are making progress with the evaluation.

I apologize for the short notice, but it occured to me that you and/or some of your folks might be interested in a training course we are giving in Reston on January 19th (syllabus attached). It is primarily for non-technical personnel, and provides tremendously valuable knowledge about how to protect yourself on the internet. I consider myself somewhat technical, and was surprised in hearing a condensed version of it the other day how many threats there are out there that I was unaware of. The course cost is $600, but for this introductory session on Jan 19th it is only $300.

You can sign up online via one of the following links:

AM Session: **http://www.suretomeet.com/exec/qt/event.h,event=bbab6e4cffab**

PM Session: **http://www.suretomeet.com/exec/qt/event.h,event=bbcb8e6c11cb**

If you or any of your colleagues sign up please let me know so I can track my efforts.

Thanks,

Best Regards,
(b)(6), (b)(7)c Business Development
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
(b)(6), (b)(7)c
www.cyveillance.com

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (CID)
Sent: Wednesday, September 29, 2010 10:30 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Pursuant to Open Source Award

(b)(6), (b)(7)c

Glad we can finally get the operational phase going. I'm not ruling out talking to (b)(4) but need to wait until we get out process working? Also, I'm going to need a little more info regarding the scope of the discussion.

(b)(6), (b)(7)c
Assistant Special Agent in Charge
Criminal Investigative Division
US Secret Service
(b)(6), (b)(7)c (off)
(cell)

From: (b)(6), (b)(7)c
Sent: Wednesday, September 29, 2010 10:24 AM
To: (b)(6), (b)(7)c
Subject: Pursuant to Open Source Award

Hi (b)(6), (b)(7)c

I hope you're doing well.

I wanted to extend my thanks to you both for your patience with us during the procurement process with so many questions, etc. This was the first large government project we've done, and the first we've done using a QNA contract, so it was a learning experience.

Also, I got a request from one of our QNA execs this morning asking if it would be possible for someone he is working with at (b)(4) to speak with one of our contacts at USSS about Cyveillance. We haven't mentioned that USSS is a customer, as we are not sure exactly what rules apply, but wanted to ask if you would be willing to arrange a conversation.

Thanks.

Best Regards,

(b)(6), (b)(7)c Business Development
Cyveillance, Inc.
World Leader in Cyber Intelligence
1555 Wilson Blvd, Suite 406
Arlington, VA 22209
(b)(6), (b)(7)c
www.cyveillance.com

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Friday, September 17, 2010 8:44 AM
To: (b)(6), (b)(7)c
Subject: RE: following up

OK thanks.

From (b)(6), (b)(7)c
Sent: Friday, September 17, 2010 8:45 AM
To: (b)(6), (b)(7)c
Subject: RE: following up

I have no idea....on either side. I've had other fish to fry for the past 2 weeks.

(b)(6), (b)(7)c
Assistant Special Agent in Charge
Criminal Investigative Division
US Secret Service
(b)(6), (b)(7)c (off)
(cell)

From: (b)(6), (b)(7)c
Sent: Friday, September 17, 2010 8:41 AM
To: (b)(6), (b)(7)c
Subject: RE: following up

Thanks (b)(6), (b)(7)c So based on your discussion has she relaxed her position at all as far as payment terms?

From: (b)(6), (b)(7)c
Sent: Friday, September 17, 2010 8:38 AM
To: (b)(6), (b)(7)c
Subject: RE: following up

Good morning,

Things are hectic as usual here -worse at the end of the year. I believe she'll be calling you soon to work through whatever issues are still on the table..

(b)(6), (b)(7)c
Assistant Special Agent in Charge
Criminal Investigative Division
US Secret Service
(b)(6), (b)(7)c (off)
(cell)

From: (b)(6), (b)(7)c
Sent: Friday, September 17, 2010 8:34 AM
To: (b)(6), (b)(7)c (CID)
Subject: following up

Hi (b)(6), (b)(7)c

Any progress with (b)(6), (b)(7)c ?

I think it is important that she understands that (b)(7)e

The technology and labor are not generally broken out into fixed costs and hourly rates. The only reason this was done for our proposal was to make the numbers fit into the existing GSA contract QNA has with USSS.

It is a bit challenging for me right now because as per the terms of the RFP only our QNA contracts officer, (b)(6), (b)(7)c can negotiate with (b)(6), (b)(7)c is not really familiar with Cyveillance services either, so we are playing a middle man game. This is why I was hoping you could influence from your side.

Thanks and please let me know as soon as you can so we can keep things moving.

Best Regards,

(b)(6), (b)(7)c Business Development
Cyveillance, Inc., a Qinetiq Company
World Leader in Cyber Intelligence
1555 Wilson Blvd, Suite 406
Arlington, VA 22209
(b)(6), (b)(7)c
www.cyveillance.com

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c
Sent: Monday, September 27, 2010 1:25 PM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Cyveillance Solutions

Excellent, thanks (b)(6), (b)(7)c am available at the following times tomorrow:

9:00 – 11:00 am
2:00 – 3:00 pm

Please let me know if there is a time within that window that fits your schedule.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c

(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406

(b)(6), (b)(7)c

Main: 1.888.243.0097
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Monday, September 27, 2010 1:20 PM
To: (b)(6), (b)(7)c
Subject: RE: Cyveillance Solutions

(b)(6), (b)(7)c

(b)(6), (b)(7)c passed me the attached email. I will be assisting in the initial workup of this project. I am out of the office for the rest of the day but will give you a call tomorrow to say hello and discuss the process going forward. Is there a time tomorrow you will not be available?

(b)(6), (b)(7)c

Assistant Special Agent in Charge
Criminal Investigative Division
US Secret Service
(b)(6), (b)(7)c (off)
(cell)

From: (b)(6), (b)(7)c
Sent: Monday, September 27, 2010 1:09 PM
To:
Cc: (b)(6), (b)(7)c
Subject: Cyveillance Solutions

Good Afternoon (b)(6), (b)(7)c
I hope you had a pleasant weekend. My name is (b)(6), (b)(7)c and I will be one of the leads on the Secret Service delivery from an account management standpoint. We are looking forward to working with you and your team and wanted to set up a preliminary call to hammer out the details of the kickoff meeting. Is there a time this week that works for you and your team? Thanks in advance.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
1555 Wilson Blvd., Suite 406

(b)(6), (b)(7)c

Main: 1.888.243.0097
www.cyveillance.com

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (CID)
Sent: Tuesday, March 02, 2010 5:58 PM
To: (b)(6), (b)(7)c
Subject: RE: question

Lets go 3/8 @ 11A....

From: (b)(6), (b)(7)c
Sent: Tuesday, March 02, 2010 11:28 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: question

We can come anytime on Monday or from 1-5 on Tuesday.

Thanks,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Tuesday, March 02, 2010 9:15 AM
To: (b)(6), (b)(7)c
Subject: RE: question

Yes....when next week would be good

From (b)(6), (b)(7)c
Sent: Tuesday, March 02, 2010 9:05 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: question

Hi (b)(6), (b)(7)c

Would it be possible to have one last meeting before this goes to procurement? We would like to get (b)(6), (b)(7)c who is (b)(6), (b)(7)c Intelligence/Surveillance/Reconnaissance at QNA/MSG involved so we can leverage her knowledge of the contracting process and Qinetiq's existing contracts to facilitate this process and discuss how we are likely to have the best chance of success.

Would it be possible for (b)(6), (b)(7)c and I to visit with you at your office in the near future?

Thanks,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Monday, March 01, 2010 9:14 AM
To: (b)(6), (b)(7)c
Subject: RE: question

Not yet.....but getting close

From: (b)(6), (b)(7)c
Sent: Monday, March 01, 2010 9:08 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: question

Understood. Should I assume we are at the point where we need to limit communications for ethical considerations?

From: (b)(6), (b)(7)c
Sent: Monday, March 01, 2010 8:54 AM
To: (b)(6), (b)(7)c
Subject: RE: question

NO need to call, for now we have what we need....I think....If something else is needed I will reach out to you
Thanks
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Monday, March 01, 2010 8:51 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: question

Hi (b)(6), (b)(7)c

Attached is the same document I sent you last week but with the correct price. I'll give you a call shortly to discuss what else we need to do the get this ready to go to procurement.

Thanks,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Wednesday, February 24, 2010 3:36 PM
To: (b)(6), (b)(7)c (CID)'
Subject: RE: question

(b)(6), (b)(7)c

Please take a look at the attached and let me know what you think. I had to make some changes from our normal proposal template so if there are any inconsistencies or typos please forgive me and let me know so I can correct them.

Thanks,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Wednesday, February 24, 2010 1:19 PM
To: (b)(6), (b)(7)c
Subject: RE: question

Shoot me an email when you are available

From: (b)(6), (b)(7)c
Sent: Wednesday, February 24, 2010 11:28 AM

To: (b)(6), (b)(7)c (CID)
Subject: Re: question

Sure,

Im at DMV right now (fun) but will be back in the office in an hour or two. Will you be available then?

From: (b)(6), (b)(7)c (CID)
To: (b)(6), (b)(7)c
Sent: Wed Feb 24 11:24:40 2010
Subject: RE: question
I need to talk about bundles/pricing, etc... when are you available

---

From: (b)(6), (b)(7)c
Sent: Wednesday, February 24, 2010 10:20 AM
To: (b)(6), (b)(7)c (CID)
Subject: question

Hi (b)(6), (b)(7)c

I know it hasn't been two weeks, but I wanted to ask, are there concerns around Sarkosy's visit to the White House in late March? With the strained relationship (to understate it) between France and Haiti, and the tremendous sympathy for Haiti worldwide, do you think (b)(7)e might would be a good idea?

Thanks,
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Wednesday, February 17, 2010 4:42 PM
To: (b)(6), (b)(7)c
Subject: RE: Pricing breakdown for Cyveillance solution

I am reviewing the Fri documents.....give me two weeks....

From: (b)(6), (b)(7)c
Sent: Wednesday, February 17, 2010 1:52 PM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Pricing breakdown for Cyveillance solution

Hi (b)(6), (b)(7)c

I left you a message yesterday afternoon but not sure it was your mailbox as it is not personalized.

Do you require any additional information at this stage?

What are next steps?

Thanks.

Best Regards,

(b)(6), (b)(7)c Business Development

Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
(b)(6), (b)(7)c
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Tuesday, February 16, 2010 11:16 AM
To: (b)(6), (b)(7)c (CID)'
Subject: RE: Pricing breakdown for Cyveillance solution

Hi (b)(6), (b)(7)c

I just had an internal discussion, and it was correctly pointed out that breaking down the pricing components is a much different exercise when dealing with a proposal which includes (b)(7)e

(b)(7)e, (b)(4)

I hope this helps.

I will give you a call this afternoon to discuss the information we have provided and anything else you may need to move forward.

Best Regards,

(b)(6), (b)(7)c Business Development
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
(b)(6), (b)(7)c
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Tuesday, February 16, 2010 8:29 AM
To: (b)(6), (b)(7)c
Subject: RE: Pricing breakdown for Cyveillance solution

No....not to that point yet

From: (b)(6), (b)(7)c
Sent: Tuesday, February 16, 2010 8:08 AM
To: (b)(6), (b)(7)c (CID)
Subject: Re: Pricing breakdown for Cyveillance solution

No problem. Before we do, is there a specific format you prefer, i.e. a type of breakdown which would make the most sense for the type of procurement we are pursuing?

From: (b)(6), (b)(7)c (CID)
To: (b)(6), (b)(7)c
Sent: Tue Feb 16 07:15:05 2010
Subject: RE: Pricing breakdown for Cyveillance solution
Please break out the cost

From: (b)(6), (b)(7)c
Sent: Monday, February 15, 2010 2:22 PM
To: (b)(6), (b)(7)c (CID)
Subject: Pricing breakdown for Cyveillance solution

Hi (b)(6), (b)(7)c

(b)(7)e, (b)(4) As discussed, you have to the option to lock in this price for three years and avoid annual price increases.

This would include:

(b)(7)e

This breaks down to:

[redacted] (b)(7)e, (b)(4)

We can put this into a formal quote with terms and conditions but I wanted to run it by you first.

I will give you a call this afternoon to discuss where we stand and what else is needed.

Thanks.

Best Regards,
[redacted] (b)(6), (b)(7)c Business Development
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
[redacted] (b)(6), (b)(7)c
www.cyveillance.com

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (CID)
Sent: Tuesday, February 16, 2010 7:35 AM
To: (b)(6), (b)(7)c (CID)
Subject: FW: Pricing breakdown for Cyveillance solution

FYI....I asked them to break out price.....also I will be working on the time-line and start-up plan....I think (b)(6), (b)(7) said she was coming over this wed, are you available

---

From: (b)(6), (b)(7)c
Sent: Monday, February 15, 2010 2:22 PM
To: (b)(6), (b)(7)c (CID)
Subject: Pricing breakdown for Cyveillance solution

Hi (b)(6), (b)(7)c

(b)(7)e, (b)(4) As discussed, you have to the option to lock in this price for three years and avoid annual price increases.

This would include:

(b)(7)e, (b)(4)

We can put this into a formal quote with terms and conditions but I wanted to run it by you first.

I will give you a call this afternoon to discuss where we stand and what else is needed.

Thanks.

Best Regards,

(b)(6), (b)(7)c Business Development
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"

(b)(6), (b)(7)c

www.cyveillance.com

(b)(6), (b)(7)c (PID)

From: (b)(6), (b)(7)c (PID)
Sent: Monday, September 26, 2011 11:01 AM
To: (b)(6), (b)(7)c
Cc:
Subject: FW: Question re: Initial Setup of USSS (b)(7)e
Attachments: USSS (b)(7)e for Cyveillance.xls; USSS Cyveillance worksheet.xls

Hi (b)(6), (b)(7)c

This is (b)(6), (b)(7)c response. It does not appear that he received anything specific from GPA or CID, other than special requests.

Thanks

(b)(6), (b)(7)c

Supervisory Protective Intelligence Research Specialist
U.S. Secret Service
Protective Intelligence and Assessment Division
Risk Management Branch
(b)(6), (b)(7)c (direct)

From: (b)(6), (b)(7)c
Sent: Friday, September 23, 2011 8:25 PM
To: (b)(6), (b)(7)c
Cc:
Subject: RE: Question re: Initial Setup of USSS Cyveillance

Hello (b)(6), (b)(7)c
My apologies for the delay. Please see the attached and have a good weekend.

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
2677 Prosperity Avenue Fairfax, VA 22031

(b)(6), (b)(7)c

Main: 1.888.243.0097
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Friday, September 23, 2011 11:40 AM
To: (b)(6), (b)(7)c

Cc: (b)(6), (b)(7)c
Subject: RE: Question re: Initial Setup of USSS Cyveillance

Hi (b)(6), (b)(7)c

Thanks for getting back to me. Would you mind forwarding me the original requirements documents submitted to you by us, GPA, and CID. We were only able to locate our draft material. I'm just looking for the lists (b)(7)e requirements.

Thanks,

(b)(6), (b)(7)c

Supervisory Protective Intelligence Research Specialist
U.S. Secret Service
Protective Intelligence and Assessment Division
Risk Management Branch
(b)(6), (b)(7)c direct)

From: (b)(6), (b)(7)c
Sent: Thursday, September 22, 2011 4:10 PM
To:
Cc: (b)(6), (b)(7)c
Subject: RE: Question re: Initial Setup of USSS Cyveillance

Good Afternoon (b)(6), (b)(7)c
All we received were the configuration documents and (b)(7)e provided by PID. Please let me know if you require access to those forms and I can definitely send them over. We have the Cyveillance-provided worksheet that you filled out and another supplemental spreadsheet provided by USSS entitled "USSS (b)(7)e for Cyveillance."

Kind regards,

(b)(6), (b)(7)c

(b)(6), (b)(7)c Cyber Intelligence Division
Cyveillance, Inc. (a QinetiQ North America Company)
"World Leader in Cyber Intelligence"
2677 Prosperity Avenue Fairfax, VA 22031

(b)(6), (b)(7)c

Main: 1.888.243.0097
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Thursday, September 22, 2011 3:35 PM
To:
Cc: (b)(6), (b)(7)c
Subject: Question re: Initial Setup of USSS Cyveillance

(b)(6), (b)(7)c

We're trying to respond to some PIA issues for our privacy officer. When Cyveillance was set up, did GPA and CID provide (b)(7)e

I don't need the actual lists, but whether they did.

Thanks,

(b)(6), (b)(7)c

Supervisory Protective Intelligence Research Specialist
U.S. Secret Service
Protective Intelligence and Assessment Division
Risk Management Branch
(b)(6), (b)(7)c (direct)

From: (b)(6), (b)(7)c
Sent: Tuesday, January 12, 2010 5:33 PM
To: (b)(6), (b)(7)c (CID)
Subject: Pursuant to yesterday's meeting

Attachments: USSS Presentation.ppt
Hello (b)(6), (b)(7)c

Sorry it took a while to get this out, we have been in meetings bell to bell today.

Thanks again for your time and attention yesterday. Please pass along my appreciation to the rest of the group.

The slides we presented are attached.

Also, I wanted to mention that (b)(6), (b)(7)c who is a new agent Secret Service as of last year, is a former Cyveillance analyst. I touched base with her and she said she would be happy to speak with you if you have questions about our company.

As requested, the following is a summary of Cyveillance's key differentiators:

(b)(4), (b)(7)e

6) We are located in Rosslyn, VA - This puts us in close proximity to USSS HQ and puts us right in the heart of the intelligence community (which is where we recruit much of our talent).

7) We offer alternate language capability

Pricing: The price range for Cyveillance services is from (b)(7)e, (b)(4) (b)(4), (b)(7)e depending on which you purchase. (b)(4), (b)(7)e If we need to customize our offering that is no problem, but the price may go up, depending on your requirements.

Please let me know what additional information I can provide to help with your evaluation.

I will call you later in the week to follow up.

Best Regards,

(b)(6), (b)(7)c
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
(b)(6), (b)(7)c FAX
www.cyveillance.com

Unknown

From: (b)(6), (b)(7)c (CID)
Sent: Thursday, January 25, 2007 8:44 PM
To: (b)(6), (b)(7)c
Subject: RE: Cyveillance

I have passed on info....they are evaluating.....

From: (b)(6), (b)(7)c
Sent: Thursday, January 25, 2007 9:32 AM
To: (b)(6), (b)(7)c
Subject: RE: Cyveillance

Hello (b)(6), (b)(7)c

I hope you're doing well. Did you have an opportunity to discuss the issue below with your team?

Thanks
(b)(6), (b)(7)c

From: (b)(6), (b)(7)c
Sent: Monday, January 22, 2007 4:52 PM
To: (b)(6), (b)(7)c
Subject: Cyveillance

Hello (b)(6), (b)(7)c

It was a pleasure to speak to you this morning. As discussed during our call, Cyveillance handles online issues for a variety of corporations and organizations. One of these issues is the problem of phishing. To combat the problem, we provide our clients a complete anti-phishing service that addresses virtually all phases of a phishing attack from prevention and detection to response and recovery.

Many of our clients wish to provide the information we obtain in the course of handling a phishing attack to the appropriate authorities to assist in potential prosecutions against these online criminals. Cyveillance, on behalf of our clients, would like to ease the process of providing this information to your Cyber Crimes Division. Can you or someone from your team help facilitate a discussion of how we could accomplish the aforementioned task? We are located in Arlington, VA, so conference calls or face-to-face meetings (here or at your office) are both easy options. I look forward to hearing back from you.

Regards,
(b)(6), (b)(7)c

(b)(6), (b)(7)c
(b)(6), (b)(7)c Product Management
Cyveillance, Inc.
(b)(6), (b)(7)c

Unknown

From: (b)(6), (b)(7)c
Sent: Friday, January 08, 2010 10:11 AM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Pursuant to our conversation yesterday

Good morning (b)(6), (b)(7)c

For Monday's appointment, (b)(6), (b)(7)c Director of Sales Operations, and myself are confirmed to visit your offices at 2pm on Monday, January 11th.

(b)(6), (b)(7)c who is our technical manager, will be joining by phone.

We will need a projector, but not internet access.

A loose agenda is as follows:

I. Introductions
II. Cyveillance Overview
II. Cyveillance Brand Intelligence
III. Q&A
IV.Next Steps

We look forward to meeting you.

Best Regards,

(b)(6), (b)(7)c Business Development
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
(b)(6), (b)(7)c FAX
www.cyveillance.com

From: (b)(6), (b)(7)c
Sent: Thursday, January 07, 2010 1:26 PM
To: (b)(6), (b)(7)c
Subject: RE: Pursuant to our conversation yesterday

I just notices that Monday is the 11th not the 12th we are scheduled for the 11th @ 2p

---

From: (b)(6), (b)(7)c
Sent: Thursday, January 07, 2010 12:17 PM
To: (b)(6), (b)(7)c (CID)

Subject: Re: Pursuant to our conversation yesterday

Sounds good. I'm out of the office today let me get back to you tomorrow with the names. What is your address?

From: (b)(6), (b)(7)c (CID)
To: (b)(6), (b)(7)c
Sent: Thu Jan 07 11:58:40 2010
Subject: RE: Pursuant to our conversation yesterday
Monday, January 12 at 2pm

From: (b)(6), (b)(7)c
Sent: Wednesday, January 06, 2010 10:23 AM
To: (b)(6), (b)(7)c (CID)
Subject: Pursuant to our conversation yesterday

Hello (b)(6), (b)(7)c

As per my voicemail, I recalled the previous message, though it may still appear in your inbox in which case please disregard.

The following are available times for us to come present at your offices next week:

Friday, January 15 at 10am or 2pm

Some questions to help us prepare:

1) What are your biggest areas of concern?

(b)(7)e

I look forward to hearing from you.

Best Regards,

(b)(6), (b)(7)c, Business Development
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
(b)(6), (b)(7)c FAX
www.cyveillance.com

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

Unknown

From: (b)(6), (b)(7)c (CID)
Sent: Thursday, January 07, 2010 4:41 PM
To: (b)(6), (b)(7)c (PID)
Subject: RE: Visible Technologies

Attachments: OpenSource Project.doc

OpenSource
Project.doc (48 KB)..

-----Original Message-----
From: (b)(6), (b)(7)c (CID)
Sent: Thursday, January 07, 2010 4:28 PM
To: (b)(6), (b)(7)c (CID)
Subject: Re: Visible Technologies

Thnx. U still da man

----- Original Message -----
From: (b)(6), (b)(7)c (CID)
To: (b)(7)c, (b)(6)
Cc: (b)(6), (b)(7)c (CID)
Sent: Thu Jan 07 15:39:52 2010
Subject: RE: Visible Technologies

2p

-----Original Message-----
From: (b)(6), (b)(7)c
Sent: Thursday, January 07, 2010 1:19 PM
To: (b)(6), (b)(7)c (CID)
Subject: RE: Visible Technologies

(b)(6), (b)(7)c we are good for the 13th - you pick the time. Looking forward to meeting.

Attending from Visible Technologies:

(b)(6), (b)(7)c Products
(b)(6), (b)(7)c Products
(b)(6), (b)(7)c

Please let me know what other information you need.

tom

(b)(6), (b)(7)c Business Development / Federal Sector Visible Technologies
mobile
(b)(6), (b)(7)c
www.visibletechnologies.com

-----Original Message-----
From: (b)(6), (b)(7)c
Sent: Wednesday, January 06, 2010 1:06 PM
To: (b)(6), (b)(7)c
Subject: RE: Visible Technologies

What time on wed, thurs

-----Original Message-----
From: (b)(6), (b)(7)c
Sent: Wednesday, January 06, 2010 4:01 PM
To: (b)(6), (b)(7)c (CID)
Subject: Visible Technologies

Hi (b)(6), (b)(7)c

I left you a voice mail this morning - I run our govt effort. (b)(6), (b)(7)c told me you talked a little while ago.

I'm based in San Francisco, but will be in DC next Wednesday and Thursday, meeting with customers. If you have some blocks of time those days, we would be happy to show you our stuff.

I'm available today and tomorrow to talk - looking forward to it.

Regards,

(b)(6), (b)(7)c
m

Sent using my Blackberry - sorry about typos.

Unknown

From: External (b)(6), (b)(7)c
Sent: Tuesday, January 05, 2010 11:16 AM
To: (b)(6), (b)(7)c (CID)
Subject: Vendor Contacts

(b)(6), (b)(7)c

See below:

Let them know that we referred you based on their interactions with us. If we can be of anymore assistance, don't hesitate.

Cyveillance:

(b)(6), (b)(7)c
Cyveillance
1555 Wilson Blvd
Arlington, VA 22209
Direct: (b)(6), (b)(7)c
Email: (b)(6), (b)(7)c
www.cyveillance.com

Visible Technologies:

(b)(6), (b)(7)c
Visible Technologies
Atlanta, Georgia 30068
direct/mobile: (b)(6), (b)(7)c
Email: (b)(6), (b)(7)c
www.visibletechnologies.com

JPMORGAN CHASE & C O .
(b)(6), (b)(7)c
Global Security & Investigations
Cyber Division
570 Washington Blvd. 7 th Floor
Jersey City, NJ 07310
|Office: (b)(6), (b)(7)c |Fax: (b)(6), (b)(7)c
(b)(6), (b)(7)c

Unknown

From: (b)(6), (b)(7)c

Sent: Wednesday, January 06, 2010 3:37 PM

To: (b)(6), (b)(7)c (CID)

Subject: Cyveillance meeting better for Friday 1-15

Attachments: (b)(6), (b)(7)c Bio Full Page 07 (2).doc

(b)(6), (b)(7)c

I have confirmed that our Cyber Intelligence Director, (b)(6), (b)(7)c, is available for the Friday 2pm time slot. Please, if possible, let's do it then because I think she brings tremendous value to the meeting.

(b)(6), (b)(7)c

Her full bio is attached as well.

Best Regards,

(b)(6), (b)(7)c
Cyveillance, Inc.
"The World Leader in Cyber Intelligence"
(b)(6), (b)(7)c FAX
www.cyveillance.com

Unknown

From: (b)(6), (b)(7)c (TSD)
Sent: Tuesday, June 03, 2003 8:28 AM
To: ecb
Cc: (b)(6), (b)(7)c
Subject: FW: Cyveillance Info.

Attachments: Homeland_Security_wp1.pdf; HomelandSecurityoverview.pdf


Homeland_Security _wp1.pdf (226...


HomelandSecurityo verview.pdf (...

Is anyone looking at this....

-----Original Message-----
From: (b)(6), (b)(7)c
Sent: Monday, June 02, 2003 5:19 PM
To: (b)(6), (b)(7)c
Subject: FW: Cyveillance Info.

Let me know what you guys think of this service. You guys in GQ may already be looking into this.

(b)(6), (b)(7)c

-----Original Message-----
From: (b)(6), (b)(7)c
Sent: Monday, June 02, 2003 3:52 PM
To:
Cc: (b)(6), (b)(7)c
Subject: Cyveillance Info.

Hi (b)(6), (b)(7)c enjoyed speaking with you. Here's some further background for you
on Cyveillance. As I mentioned, for our financial customers we find 8 to 10
thousand stolen credit cards every day on the Internet. About 10% of these
have social security numbers associated with them.

The white papers I am attaching address themselves to terror oriented Homeland security applications.

Thx. (b)(6), (b)(7)c I'll be in touch soon.

(b)(6), (b)(7)c
Cyveillance
(b)(6), (b)(7)c

. <<Homeland_Security_wp1.pdf>> <<HomelandSecurityoverview.pdf>>

Cyveillance

100% Relevant Intelligence™

Homeland Security

A Cyveillance White Paper

October 2002

RIF

The Situation

One of the highest priorities of the Government is the investigation of foreign intelligence, terrorist, and criminal activities that directly threaten the homeland security of the United States. Government agencies must identify, prevent and defeat threats to homeland security before they occur. Terrorists actively use the Internet to proselytize, recruit members, gather intelligence and plan attacks. Government agencies need leading-edge technology that will leverage the Internet as a homeland security resource and keep them one step ahead. Rapidly collecting and analyzing the massive volume of online, open source intelligence presents an opportunity to further enhance the effectiveness in detecting and stopping threats to homeland security.

Cyveillance understands that the Government does not have the time or resources to sift through billions of documents on the Internet trying to identify hidden risks, unforeseen threats or fraudulent activity. The immense density and compartmental nature of the Internet makes it nearly impossible for Government agencies to cost-effectively extract, categorize, prioritize, and analyze this information on their own. To effectively harness this unstructured mass of data, a comprehensive solution and robust technology are needed to separate the noise from the true intelligence. Cyveillance is solely focused on this aim. Cyveillance's proprietary Internet intelligence technology can help Government agencies achieve their homeland security objectives.

Cyveillance Intelligence Center Technology

Cyveillance has developed and deployed technology for the collection and analysis of Internet intelligence on behalf of leading corporations around the world for commercial purposes. The Cyveillance Intelligence Center (CIC) technology provides an ideal foundation to quickly configure a derivative platform for investigative purposes.

Volume, Variety and Velocity

Effective Internet intelligence means collecting, processing, categorizing, and prioritizing massive volumes of data quickly. This requires state-of-the-art technology that can rapidly analyze unstructured data found on the Internet or other sources. CIC technology's ability to identify the most relevant information will allow Government analysts to spend their time analyzing true intelligence and eliminate the need to manually surf through unmanageable amounts of data for investigative leads. A high-level overview of the system is described below:

Data Collection

CIC intelligent agents and highly efficient downloaders provide around-the-clock monitoring of the Internet. They pour through all publicly available online sources evaluating unstructured content and breaking down HTML code. The crawlers and

intelligent agents recognize relevant multi-language text, images, software, audio and video. CIC technology's ability to crawl a diverse set of Internet protocols and process virtually all forms of content represents close to 100% coverage of the Internet. And, because the technology does not depend on commercial search engines, which cover only select protocols and a small overall percentage of the Internet, the Government will achieve superior coverage.

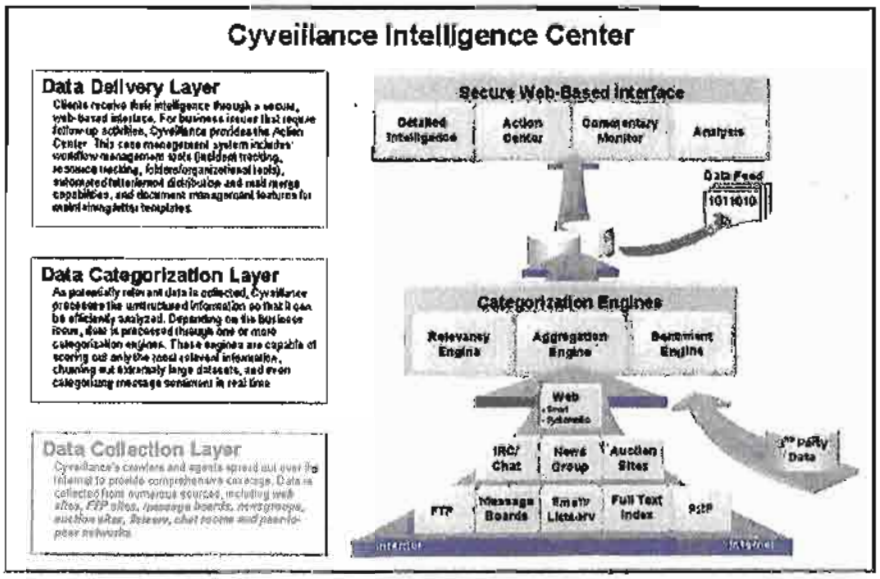
Cyveillance employs both a systematic and smart crawl of the web. The systematic crawler ensures every site is revisited regularly while the smart crawler follows links where client-relevant content is present.

Data Categorization and Prioritization

Once suspect content is identified, CIC categorization engines structure, score, and add additional context to extract a meaningful dataset, from which to filter and sort the information acquired and prioritize the findings. The engine is designed to accommodate artificial intelligence and decryption capabilities. Context is added by categorizing important details about the content, after which relevancy scoring algorithms will be applied to identify the highest priority content. The scoring algorithms are user-configurable and specific to CIC issues so that only the most actionable, high-impact content is delivered for final human analysis. The flexible, user-friendly configuration will accommodate both on-going monitoring efforts as well as ad-hoc investigative queries.

Data Delivery

The CIC aggregates third party data sources, including Internic registration details or information from other sources. The system will disseminate the complete dataset to the appropriate personnel for expert review and analysis. The intelligence will then be organized and disseminated based on user-defined configurations, such as a specific issue, content, language or other issues of interest. Archives will be maintained for investigative queries that require analysis of historical content and as a repository for forensic evidence.



RIF

Coverage

Currently, CIC provides coverage of the most widely used protocols that make up the Internet. If enhanced, the technology can process additional offline data sources through its categorization engines.

In addition to the breadth of coverage, the speed and depth of the system can be configured to meet the needs of Government agencies. The following is a categorization and breakdown of the areas of the Internet that would likely be of the most value for gathering intelligence pertaining to homeland security issues:

Global Information Sources

- World Wide Web
- File Transfer Protocol
- Message boards

Searchable feeds

- Usenet
- Online news sources

Community-Based Information

- Internet Relay Chat (IRC) Channels
- Email-based discussion forums and Spam

Searchable Databases

- Search engines
- Auction sites
- Registration information

Cyveillance Coverage

Cyveillance crawls over 40 million domains every month.

IRC agent monitors conversations with context.

Over 10,000 emails processed each day.

Cyveillance monitors both open and closed peer-to-peer networks.

In addition to using its own crawlers, Cyveillance accesses over 2.1 billion pages of coverage through strategic partnerships.

Homeland Security Applications

CIC technology will immerse the Government in the same digital environment in which individuals and organizations that threaten homeland security already operate. Not only will this allow for the detection of threats to national security and other criminal activity, but it will also enable Government agencies to monitor and exploit information available over the Internet, giving them the ability to detect vulnerabilities and influence criminal activities.

While potential CIC applications for homeland security issues are very broad, the following are some examples of how it might be applied:

- Collection of intelligence on key adversary or terrorist organizations and their activities, including monitoring specifically for threats, conspiracies, or planned attacks against US interests.

Cyveillance
Minding your business on the Net

RIF

For over 5 years, large commercial companies have been relying on Cyveillance technology.

- Monitoring for leaks of confidential information or content that heightens risk, such as specifications on airplanes, airport security details, bomb-making instructions, biohazards, blue prints, itineraries, security details, etc.
- Monitoring for threats or suspicious activities associated with critical infrastructure targets or events of national significance.
- Monitoring for threats or other indication of planned cyber attacks in the form of hacks, denial of service, etc.
- Conducting ad-hoc queries and collecting evidence in support of state, local and international law enforcement partners.
- Periodic checks and monitoring for any online content that could pose a risk to backstops created to ensure the safety and security of undercover agents.
- Collection of intelligence on organized crime activities.

As these examples illustrate, the CIC would further enhance the effectiveness of Government agencies on many fronts. Internet intelligence will better position the Government to achieve its strategic objectives and arm agencies with a technology to give them the upper hand in detecting and responding to threats to homeland security.

Clients Using CIC Technology

CIC technology has helped numerous clients manage the risks and opportunities available to them on the Internet. Cyveillance's unique capability of providing close to 100% Internet coverage and delivering only highly relevant information ensures clients receive only the most pertinent information; information that directly impacts their ability to protect their company and their customers. The solutions Cyveillance provides range from assisting organizations in managing threats against their property and personnel to monitoring for fraudulent use of their products. Cyveillance technology excels in taking large volumes of data and extracting the most important pieces to facilitate further understanding and protection of its clients. Examples of the types of services provided to Cyveillance clients are included below.

Global Pharmaceutical Manufacturer (under NDA)

Corporate Security Management

Since 1998 Cyveillance has provided Internet intelligence to one of the largest research-based, global pharmaceutical companies. Cyveillance uses its technology and experience to search for threats to this global company's security. Cyveillance has returned highly relevant data to this company on a range of security issues, including leaks of proprietary product information, organized extremist activities against the Company, employee discussion of issues that pose a security threat, and financial message board postings that contain inside information. Cyveillance's ability to provide this information in a timely manner allows the corporate security officers to protect their company's financial interests, while allowing the rest of the company to focus on their core mission.

Cyveillance counts 1 of the ortune 0 as clients

Home Depot

Boycott Identification

Cyveillance monitored Usenet and Newsgroup communities to identify several specific issues for Home Depot, including commentary from environmentalists, disgruntled employees and others that were planning boycotts against Home Depot. As the Internet is increasingly used as a method of communication and community building, boycott organizers used this medium to coordinate their efforts. Cyveillance was able to keep alert for brewing boycotts and notify Home Depot of these potential threats. This allowed Home Depot to increase security to ensure their consumers and employees were protected from potential problems. Cyveillance technology allowed Home Depot to proactively address evident risks and prevent significant and costly negative PR situations as well as minimize associated revenue losses.

Consumer Products Division, Major Pharmaceutical Company (under NDA)

Illegal Product Distribution

The health care products division of a major pharmaceutical company sought Cyveillance's services due to concern over the illegal sale and distribution of several of their products. In particular, they were interested in sites offering expired or institutional products to consumers. Products that are stolen or sold to unauthorized distributors can be easily sold online far past the products' intended expiration date, thus creating major liability risks. In addition, the sale of institutional products, which are packaged differently and sold at a lower cost, presents brand liability risks and revenue leakage. Finding these sites on the Internet is a difficult task, as they are disseminated widely across the billions of pages of the web, and timeliness is essential to shutting the illegal activity down. After engaging Cyveillance to search the web for these specific sites, it was determined approximately 20% of the retail sites selling this company's product were selling expired or institutional products. Cyveillance is continuing to closely track online sales for this client, enabling them to better control their distribution channel, and limit the liability generated from illegal sales.

Merrill Lynch

Personnel/Company/Intellectual Property Threats

Merrill Lynch sought Cyveillance out to provide protection for their intellectual property online. As Merrill Lynch produces highly valuable content and possesses a universally recognized name, sites take advantage of these assets and claim authenticity by being associated with the company. In addition, Merrill Lynch asked Cyveillance to monitor for threats against the safety and security of analysts and the company as a whole. Cyveillance uses its far reaching crawlers and its categorization ability to filter out the numerous mentions of Merrill Lynch that are not relevant to the protection of their analysts, company, or intellectual property in order to deliver only the most pertinent sites to Merrill Lynch for further review.

RIF

Cyveillance
Minding your business on the Net

Accessing The Technology

Several delivery hosting and delivery options are available to service the Government's homeland security needs. Cyveillance can work with Government agencies to select one of the outlined options, or further define a delivery methodology that best meets their specific needs. Options for delivery include:

Option 1: Cyveillance houses the collected data in its own data warehouse, similar to the delivery methodology used for existing clients. In this option data collection and analysis occurs at Cyveillance's secured location.

Option 2: Cyveillance provides the collected data through a secure network. In this scenario, data collection would occur at Cyveillance's facility, while all categorization and programmatic analysis would occur at agency-specified locations.

Option 3: Cyveillance provides an enhanced security option by replicating its data collection, analysis, and categorization technologies at secure government locations. Deploying the system in a number of locations around the world would yield a fault tolerant and heavily redundant evidence extraction and analysis tool.

Option 4: Cyveillance licenses its source code. Cyveillance provides developer support to each agency's development teams and together builds an autonomous data collection and analysis application run at the agency's location and on agency hardware. The agency's infrastructure would provide the support function.

A Cyveillance support team is made available throughout the delivery process to ensure that delivery of information continuously meets each agency's expectations. The Cyveillance support team will work with each agency to understand its specific needs and requirements as they relate to Internet intelligence. This information will be used to program Cyveillance technology to address those needs.

Cyveillance, Inc.

Cyveillance has emerged as a first line of defense for the online detection of security issues, and for this reason has become a close ally of numerous traditional, offline security firms. Founded in 1997, the company has 19 of the Fortune 50 as clients, along with numerous other companies deemed leaders in their field of expertise. Over the past five years, Cyveillance has developed and refined an advanced technology capable of transforming massive volumes of data into filtered, pertinent intelligence. It is this capability that Cyveillance will use to help the Government identify potential and existing homeland security threats.

Cyveillance helps organizations address critical security and business issues by delivering 100% Relevant Internet intelligence mined directly from the Internet. The company's solutions enable organizations to heighten awareness and take control of their presence online. Cyveillance provides a complete solution to many well-known clients. These clients have selected Cyveillance for its unique technological capabilities and experienced personnel.

Cyveillance configures its proprietary technology with client-specific parameters to locate and categorize unstructured content, transforming the Internet into a critical resource for strategic analysis. Cyveillance's hosted solutions are available in multiple languages and designed to serve its growing list of Global 2000 organizations.

Cyveillance
Minding your business on the Net
.cyveillance.com

Headquarters
1555 Wilson Boulevard
Suite 404
Arlington, VA 22209-2405
Tel: 703.351.1000
Fax: 703.312.0536

UK Distributor
New Vantage, Ltd.
Cannon Street
London
C N N
Tel (0) 0 0 0
a (0) 0 001

RIF

Homeland Security

Have the Front Lines of Homeland Security Been Left Unguarded on the Internet?

One of the highest priorities of the Government is the investigation of foreign intelligence, terrorist, and criminal activities that directly threaten the homeland security of the United States. Terrorists actively use the Internet to proselytize, recruit members, gather intelligence and plan attacks. The immense density and compartmental nature of the Internet makes it nearly impossible for Government agencies to cost-effectively extract, categorize, prioritize, and analyze this information on their own. Cyveillance is solely focused on this aim. Cyveillance's proprietary Internet intelligence technology can help Government agencies achieve their homeland security objectives.

While potential Cyveillance technology applications for homeland security issues are very broad, the following are some examples of how it might be applied to be of most value to the Government:

- Collection of intelligence on key adversary or terrorist organizations and their activities, including monitoring specifically for threats, conspiracies, or planned attacks against US interests.
- Monitoring for leaks of confidential information or content that heightens risk, such as specifications on airplanes, airport security details, bomb-making instructions, biohazards, blue prints, itineraries, security details, etc.
- Monitoring for threats or suspicious activities associated with critical infrastructure targets or events of national significance.
- Monitoring for threats or other indication of planned cyber attacks in the form of hacks, denial of service, etc.
- Conducting ad-hoc queries and collecting evidence in support of state, local and international law enforcement partners.
- Periodic checks and monitoring for any online content that could pose a risk to backstops created to ensure the safety and security of undercover agents.

Cyveillance has emerged as a first line of defense for the online detection of security issues, and for this reason has become a close ally of numerous traditional, offline security firms.

Cyveillance helps organizations address critical security and business issues by delivering 100% Relevant Internet intelligence mined directly from the Internet. The company's solutions enable organizations to heighten awareness and take control of their presence online. Cyveillance configures its proprietary technology with client-specific parameters to locate and categorize unstructured content, transforming the Internet into a critical resource for strategic analysis. Cyveillance's hosted solutions are available in multiple languages and designed to serve its growing list of Global 2000 organizations.

For More Information ▶

Cyveillance, Inc.
Call: 1.888.243.0097
Email: info@cyveillance.com
Visit: www.cyveillance.com

UK Distributor
New Vantage, Ltd.
Dial: +44 (0)20 7556 7040
Email: info@newvantage.co.uk
Visit: www.newvantage.co.uk

www.cyveillance.com

Unknown

From: (b)(6), (b)(7)c (SAV)
Sent: Friday, November 07, 2003 4:07 PM
To: (b)(6), (b)(7)c
Subject: FW: Cyveillance Presentation
Attachments: CorpOverview.pdf; CySecurityCards.pdf; CySecurityIdentity.pdf; Identity_Theft.pdf


CorpOverview.pdf (163 KB)


CySecurityCards.pdf (115 KB)


CySecurityIdentity.pdf (131 KB...


Identity_Theft.pdf (386 KB)

I have scheduled a presentation for Wednesday, 11/12/03, at 2 PM in the CID conference room. Please make an effort to attend.

-----Original Message-----
From: (b)(6), (b)(7)c
Sent: Wednesday, November 05, 2003 4:16 PM
To: (b)(6), (b)(7)c
Subject: Information per our conversation

Thank you for taking the time to talk with me today. Per our conversation, I am sending information regarding our technology for your review. I have attached a link to our website, as wells as, white papers to this e-mail. We have developed a system (b)(7)e The core benefit to our system is actionable intelligence that can be used by U. S. Secret Service proactively target;

* Credit Card Fraud
* Financial Crime associated with Identity Theft

I look forward to meeting with you and your management team on Wednesday November 12th, at 2:00 p.m. to present how we can improve your capabilities and enhance the execution of the U.S. Secret Service mission. I will call you Friday to confirm. Should you have any questions, please call me at (b)(7)c, (b)(6)
Please feel free to send this e-mail to other members of your team.
Thank you for your assistance.

(b)(6), (b)(7)c
Cyveillance, Inc.
o) (b)(6), (b)(7)c
c) (b)(6), (b)(7)c
www.cyveillance.com

<<CorpOverview.pdf>> <<CySecurityCards.pdf>> <<CySecurityIdentity.pdf>> <<Identity_Theft.pdf>>

Cyveillance

100% Relevant Intelligence™

Cyveillance Corporate Overview

Company Snapshot

Cyveillance, the leading provider of 100% Relevant eBusiness Intelligence™, provides Global 2000 organizations with high-impact, actionable intelligence drawn from—and delivered securely over—the Internet. Cyveillance configures its proprietary technology with client-specific parameters to locate and categorize unstructured content, transforming the Internet into a critical resource for increasing revenue, improving operational efficiencies and mitigating mission-critical risk.

Application examples of Cyveillance eBusiness Intelligence include:

- A major pharmaceutical manufacturer manages risk by monitoring for gray market sales of their product online. Expired drugs are being sold outside of distribution channels, creating significant liability while exposing consumers to risk.
- A leading hotel chain recaptures revenue being lost to unscrupulous web sites illegally using their brand.
- Numerous stock exchanges worldwide recapture lost royalty revenue by identifying unauthorized sites displaying their market data.
- Leading card-issuing banks monitor the Internet for compromised credit and debit card data.
- Top insurance companies gain awareness of how their brand is being portrayed by independent agents who are out of compliance with corporate guidelines.
- Multi-national corporations are provided eBusiness Intelligence that allows insight to potential class-action lawsuits, demonstrations and threats to officers.
- Fortune 500 General Counsels and law firms are provided intelligence and case management tools that identify IP infringement across the entire web, including international domains (ccTLDs).

"Cyveillance is always a half step ahead of us ... always thinking ahead to new ways to improve the service and give us better value."

- Interactive Marketing Director, leading multi-national insurance company

Cyveillance lists 20 of the Fortune 50 as customers.

The company, founded in 1997 and based in Arlington, Virginia, has become recognized as providing unique "must have" solutions, critical in today's economic business climate. Concurrently, as the need increases for greater revenue as well as awareness of potential risk in both corporate and government organizations, Cyveillance—with its comprehensive technology—is able to draw invaluable client-specific insights from activity occurring across billions of web pages and other Internet protocols.

Cyveillance solutions are typically offered on an annual subscription basis.

Cyveillance Technology

"We've seen a lot of technology presented to us, but yours is one of the few technologies I have seen that has a true business application."

- eCommerce executive, leading financial underwriting institution

The tremendous size and dynamic nature of the Internet make it impossible to monitor without specialized technology. To provide 100% Relevant eBusiness Intelligence, Cyveillance uses patented technology designed exclusively for this purpose. Developed and refined over a period of six years, it monitors a comprehensive set of online sources and protocols and is acutely capable of extracting true intelligence from the unstructured data that comprises the Internet.

Cyveillance technology consists of four layers:

Infrastructure: A distributed, highly scalable, enterprise-class infrastructure

Data Extraction: Intelligent, high speed data extraction agents

Transformation Engines: Deliver 100% relevant data based on custom-configurable criteria

Productivity Tools: Secure, flexible intuitive user applications for managing eBusiness Intelligence, all available 24x7 through the Cyveillance portal

Why Our Customers Buy

Revenue Generation

Increase site traffic/eliminate diversion
Recapture lost licensing revenues
Identify new sales prospects
Eliminate counterfeit distribution
Stop gray market distribution

Cost and Operational Efficiency

Eliminate manual data collection
Eliminate manual data review
Automate follow up actions
Improve case worker collaboration

Mission-Critical Risk Management

Detect corporate threats outside firewall
Protect and manage reputation
Protect Intellectual Property
Identify compromised credit and debit cards

Who Buys What

"Your product is certainly worth its weight in gold."

- Internet Channel Group, leading Canadian bank

Corporate Counsel

CyWebWatch Domains

An enterprise-strength cybersquatting protection solution that provides 100% coverage of all global and country code-level domains.

CyWebWatch Combo

A unique brand protection solution that, in addition to the capabilities of CyWebWatch Domains, provides 100% coverage of every web home page—often where the most egregious violations occur.

CyWebWatch Pro

A "white glove" brand protection service that is customized to meet each client's brand priorities and provides complete coverage of the entire web.

Cyveillance
Minding your business on the Net

RIF

CyWebWatch Piracy

CyWebWatch Piracy helps companies recapture revenue otherwise lost due to online piracy of their copyrighted materials.

VP eBusiness

CyMarketplace Compliance

CyMarketplace Compliance allows companies to increase revenues through proactive management of online partner relationships. The solution delivers information on existing partners impacting revenue and brand equity through non-compliance.

CyMarketplace Pro

CyMarketplace Pro helps companies recapture revenues by thwarting online sales of counterfeit product and unauthorized online product distribution.

CyMarketplace Re-Brand

CyMarketplace Re-Brand identifies the most critical online instances of outdated branding. By delivering the most relevant sites containing outdated branding, clients can cost-effectively improve brand consistency online and ehance brand equity.

Chief Security Officer

CySecurity Pro

CySecurity Pro monitors the Internet for company-specific threats and promptly reports them to help organizations effectively manage risks. This includes fraud, physical threats, activism and legal challenges.

CySecurity Cards

CySecurity Cards helps companies reduce fraud claims by monitoring the Internet for compromised credit and debit card numbers.

"We are kicking a#! with this thing!"

- Law Division, leading Wall Street financial services firm

Customer-Specific

Cyveillance offers eBusiness Intelligence for specific and unique customer needs. This includes reputation management, the modeling of registries, lead generation and Federal.

If you would like more information about Cyveillance solutions, please contact us today to speak to a representative. 1-888-243-0097 or direct 703-351-1000.

Cyveillance
Charting your business on the Net

1555 Wilson Boulevard
Suite 404
Arlington, VA 22209-2405

Tel: 703.351.1000
Fax: 703.312.0536
www.cyveillance.com

RIF

Cyveillance

100% Relevant Intelligence™

CySecurity Cards

A Unique Data Source to Combat Fraud

CySecurity Cards helps companies reduce fraud claims by monitoring the Internet for compromised credit and debit card numbers. Card numbers are logged and daily data files are provided to clients for further review and import into internal fraud monitoring systems. Enabled by quick identification and delivery of credit or debit card numbers found online, companies can more effectively protect their customers and minimize fraud expenses.

The Cybersource 2002 Online Fraud Report indicates merchants are losing on average 3% of online revenues to fraud.

The Impact of Online Card Fraud

The Cybersource 2002 Online Fraud Report indicates merchants are losing on average 3% of online revenues to fraud. The same report also indicated 22% of merchants report an even more serious fraud problem, with 5% of revenues lost. Banks and credit unions issuing credit and debit cards, as well as the major card companies such as Visa and Mastercard, suffer financial losses due to the theft and dissemination of card numbers in the online environment. Consumers also bear the cost in time and effort to remove fraudulent charges from their record, or to repair a damaged credit rating. Early detection of online fraud can help limit damage to all parties involved.

Data Extraction Agents Provide Unparalleled Coverage

In order to thwart online fraud and limit financial losses, Cyveillance employs a series of high-speed extraction agents to continuously monitor online sources and protocols where credit card numbers are found, traded and sold. These include:

- IRC/Chat Rooms: Users directly share card information or provide links to sites where cards can be found.
- World Wide Web: Discussions or links to sites with card information.
- Usenet: Postings that include card numbers or links to site with card information.
- FTP: Sites with listings of card numbers.

Cyveillance employs a series of high-speed extraction agents to continuously monitor online sources and protocols where credit card numbers are found, traded and sold.

Any discussions or postings containing credit card numbers from these sources are logged. Parsing technology is used to extract specific card numbers and associated information such as the issuing bank, card type, country of issue and date detected.

Daily Deliveries Improve Response Time

Each day, Cyveillance provides an encrypted data file containing the card numbers and related data collected over the past 24 hours. These files contain only client-relevant cards, typically based on BIN number.

Cyveillance
Minding your business on the Net

RIF

Enterprise-Class Infrastructure Ensures Customer Data is Secure

Cyveillance takes great steps to secure client data. Enterprise-class storage systems are backed-up daily and stored off site at a Department of Defense certified location. Cyveillance's onsite data center is protected by third-party managed security services, including intrusion detection and incident response. Industry standard firewalls, client access control mechanisms and a variety of other measures are used to protect all Cyveillance subsystems and, consequently, client data. Data security between Cyveillance and its clients is also a central focus therefore the Cyveillance online case management system is equipped with SSL.

About Cyveillance

Cyveillance has emerged as the leader in eBusiness Intelligence by providing services to Global 1000 companies. Cyveillance delivers high-impact, 100% relevant, actionable intelligence, drawn from—and delivered securely over—the Internet. Cyveillance's Intelligence helps customers increase revenues, reduce costs, improve operational efficiencies and mitigate mission-critical risk.

Cyveillance
Minding your business on the Net

1555 Wilson Boulevard
Suite 404
Arlington, VA 22209-2405

Tel: 703.351.1000
Fax: 703.312.0536
www.cyveillance.com

REF

Cyveillance

100% Relevant Intelligence™

CySecurity Identity

Protect Your Customers from Online Fraud

CySecurity Identity helps companies quickly identify online scams misleading customers through fraudulent use of their corporate identity. By continuously monitoring the Internet, Cyveillance is able to find these online schemes in a timely manner. Companies can then take immediate action to alert and protect their customers from fraud.

One of the newest online scams uses a combination of spoofed junk email and fake storefronts to harvest personal information from unwitting consumers.

A Rapidly Growing Problem

One of the newest and most effective online scams uses a combination of spoofed junk (spam) email and fake storefronts to harvest personal information from unwitting consumers. The scenario is sometimes called phishing, brand spoofing or corporate identity theft. Regardless of what it's called, the customers of many well-known companies have fallen victim to this latest form of online fraud, including Best Buy, Sony, and Bank of America.

Cyveillance's automated technology continuously monitors junk email, new domain registrations, and the World Wide Web for indications that corporate identity theft is occurring. When suspect email messages or web sites are identified, the content is analyzed and embedded links are followed to uncover the details of the scheme. Clients are immediately alerted, enabling them to take the appropriate actions.

Through early identification of corporate identity theft schemes, CySecurity Identity allows businesses to:

- Protect customers from online fraud and personal identity theft
- Avoid negative customer experiences and brand damage associated with corporate identity theft

An Environment So Vast that Technology Is the Only Answer

It is impossible to monitor the Internet for cases of corporate identity theft using manual methods or search engines designed for different purposes. That is why Cyveillance has designed and developed a unique, proprietary technology platform to extract, transform and deliver intelligence from millions of junk email messages, over 5 billion web pages, and the thousands of new domain registrations that occur each day.

Cyveillance continually moniotrs junk email, new domain registrations, and the World Wide Web for indications that corporate identity theft is occurring.

Data Extraction Agents Provide Unparalleled Coverage

To ensure comprehensive coverage, Cyveillance employs a series of high-speed extraction agents to monitor online sources. Primary sources monitored to identify corporate identity theft include:

- **Junk email** - Cyveillance extraction agents continuously process hundreds of thousands of email messages each day to find cases of spoofed identities.
- **World Wide Web** - Cyveillance extraction agents crawl billions of web pages to identify any false storefronts masquerading as legitimate sites.
- **New Domain Registrations** - Cyveillance extraction agents continuously monitor for suspicious new domain registrations - a particularly effective method for identifying fraud schemes before they've had a chance to occur.

CySecurity provides daily reports that summarize any suspicious Internet activity.

Proprietary Data Transformation Engines Deliver 100% Relevant Intelligence

Patented Cyveillance Intelligence Center Technology delivers only those incidents relevant to the fight against corporate identify theft. Cyveillance employs its Relevancy Engine to eliminate false positives. A dedicated Cyveillance client manager configures the Relevancy Engine to meet specific customer requirements. And as needs change, the Relevancy Engine is reconfigured to meet business objectives.

Daily Reports and Immediate Alerts Keep You Informed

CySecurity Identity provides daily reports that summarize any suspicious Internet activity, particularly new domain registrations that may indicate future corporate identity theft plans. And, when a case of corporate identity theft or email spoofing is discovered, a dedicated Cyveillance client manager provides immediate notification.

Enterprise-Class Infrastructure Ensures Customer Data is Secure

Cyveillance takes great steps to secure client data. Enterprise-class storage systems are backed-up daily and stored off site and at a Department of Defense certified location. Cyveillance's onsite data center is protected by third-party managed security services, including intrusion detection and incident response. Industry standard firewalls, client access control mechanisms and a variety of other measures are used to protect all Cyveillance subsystems and, consequently, client data. Data security between Cyveillance and its clients is also a central focus therefore the Cyveillance online case management system is equipped with SSL.

About Cyveillance

Cyveillance has emerged as the leader in eBusiness Intelligence by providing services to Global 1000 companies. Cyveillance delivers high-impact, 100% relevant, actionable intelligence, drawn from—and delivered securely over—the Internet. Cyveillance's Intelligence helps customers increase revenues, reduce costs, improve operational efficiencies and mitigate mission-critical risk.

Cyveillance
Minding your business on the Net
1555 Wilson Boulevard
Suite 404
Arlington, VA 22209-2405
Tel: 703.351.1000
Fax: 703.312.0536
www.cyveillance.com

RIF

Cyveillance

100% Relevant Intelligence™

Corporate Identity Theft

How to Protect Your Organization

A Cyveillance White Paper

Prepared by:
Brian H. Murray, Cyveillance, Inc.

October 2003

RIF

Executive Summary

Corporate identity theft is a rapidly growing problem on the Internet that threatens corporations and consumers alike. Also referred to as "spoofing" or "phishing," corporate identity theft happens when an unauthorized group or individual pretends to be a well-known company. The perpetrator typically uses a fraudulent spam email or website to trick unsuspecting customers into sharing personal information such as bank account and credit card numbers. Sony, Bank of Montreal, Best Buy, UPS, and Citibank are just a few examples of companies who have recently found themselves and their customers the victims of corporate identity theft.

While the practice of corporate identity theft is burgeoning, many organizations don't understand how or why the crime is perpetrated, and aren't sure what to do about it. Fortunately, a number of insights and best practices have emerged from those companies that have been affected. The purpose of this white paper is to expose common tactics that criminals use to perpetrate corporate identity theft, and to arm companies with the knowledge necessary to protect themselves.

Background

The FTC estimates that identity theft cost consumers and businesses $53 billion in 2002.

Identity theft is a well-publicized problem that has affected many people and continues to get worse. In fact, the FTC estimates that identity theft cost consumers and businesses $53 billion in 2002. What some people don't realize is that identity theft is targeted not only at consumers, but it's also an offense directed at businesses; corporate identity theft occurs when criminals use a trusted brand for their own purposes, posing as a recognized business entity.

There are many reasons why corporate identity theft is committed, but the most common motive is to steal personal information or otherwise defraud a business' customers. Personal information harvested by identity thieves can then be used to perpetrate identity theft against individuals, contributing to the broader consumer problem.

The practice of corporate identity theft is not a new one—it has existed online since the inception of the Internet. In previous years, fewer companies were affected and, as with many security breaches, corporate victims were reluctant to publicize incidents for fear of undermining customer confidence. Today, numerous corporate identity attacks occur daily and, while some companies are more vulnerable than others, anybody could be the next target.

The pervasiveness of corporate identity theft can be attributed to many reasons, not the least of which are technology and broader Internet adoption.

Unfortunately, posing as a reputable company in the digital world is alarmingly easy. Erecting a seemingly legitimate corporate web page can be as simple as copying and pasting source code from the real thing. The crime of corporate identity theft has also been attractive to criminals because the Internet affords the anonymity and mobility to perpetrate fraud with little fear of recrimination. As with many other Internet-based crimes, technological advances have outpaced legislation and enforcement.

In response to the recent growth in corporate identity theft, both Government and the private sector have begun to dedicate resources to address the problem, and have had some early successes. There is a new sense of urgency, and more of the companies affected are fighting back. In the process, these companies have gained insights into the tricks used by criminals, and have learned how best to manage the risk. These key learnings can help you to implement processes to protect yourself and your customers should you be attacked, and potentially avoid an attack altogether.

The Costs of Corporate Identity Theft

Corporate identity theft is an attack focused directly at the heart of any successful business: their customer base.

The business implications of corporate identity theft are significant—it is an attack focused directly at the heart of any successful business: their customer base. When a business' own brands are used to defraud their loyal customers it should be an affront to every employee, and combating this activity should be a priority at every level of the organization. In fact, how a company prepares for and responds to such an offense is a good gauge of how customer-focused they truly are.

Not only does a company have a moral obligation to protect their customers, but they have a fiduciary responsibility as well. Corporate identity theft attacks can alienate loyal customers, undermine confidence, and destroy brand equity. In fact, identity theft is now being perpetrated to the point where it threatens to undermine broader confidence in e-Business.

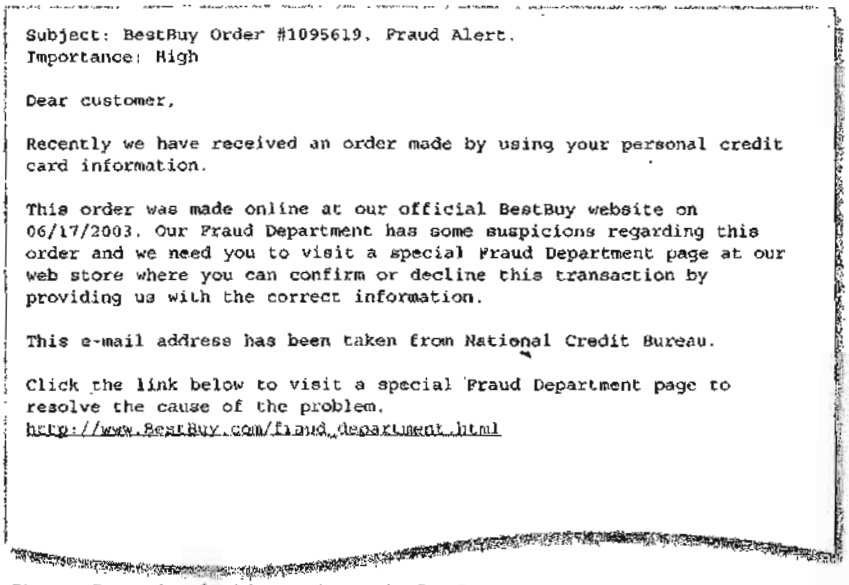
In addition to these "soft" costs, there is the direct impact of revenue loss resulting from estranged customers who are unwilling to conduct further business through the online channel or at all with that company. In some cases the businesses can also be the ones defrauded. For example, if a phony storefront collects account information that is used to purchase goods from the legitimate store, the merchant will likely end up bearing the costs of the goods shipped.

The impact of identity theft can spiral out of control if it goes un-addressed. "Looking the other way" is not a viable option.

Finally, businesses targeted by corporate identity thieves incur the administrative costs of associated customer service issues and public relations. Because identity theft is a hot issue and one that affects a lot of people, its impact can spiral out of control if it goes un-addressed and word spreads. "Looking the other way" is not a viable option.

How Corporate Identity Theft Works

There are many ways that corporate identity theft can occur on the Internet, but almost all of them are variations of luring a business' customers to a phony destination that appears to be legitimate. The premise by which the customers are enticed and the vehicle of communicating with the customer can both vary, as can the end destination. Some online messages may lure customers to send personal information by FAX or phone, but the use of websites is far more prevalent.



Subject: BestBuy Order #1095619, Fraud Alert.
Importance: High

Dear customer,

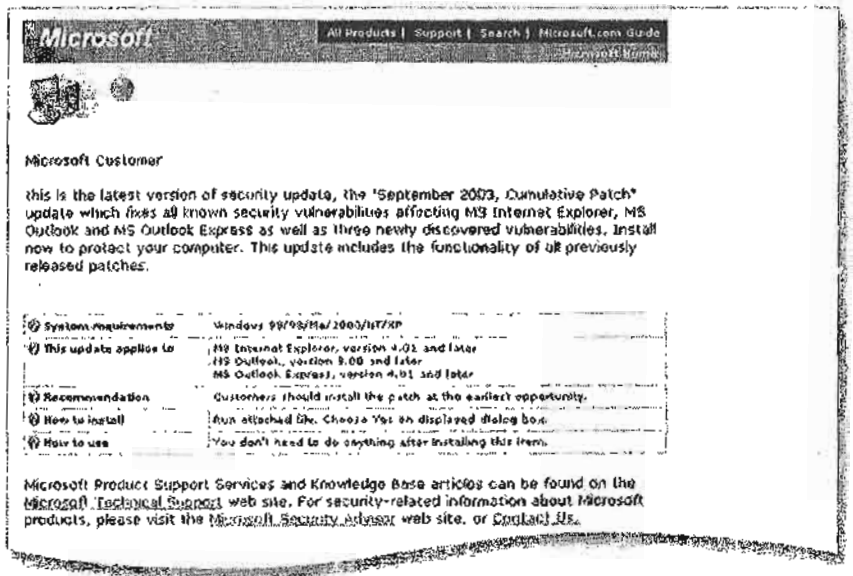
Recently we have received an order made by using your personal credit card information.

This order was made online at our official BestBuy website on 06/17/2003. Our Fraud Department has some suspicions regarding this order and we need you to visit a special Fraud Department page at our web store where you can confirm or decline this transaction by providing us with the correct information.

This e-mail address has been taken from National Credit Bureau.

Click the link below to visit a special Fraud Department page to resolve the cause of the problem.
http://www.BestBuy.com/fraud_department.html

Figure 1. Excerpt from fraudulent email targeted at Best Buy customers.



Microsoft | All Products | Support | Search | Microsoft.com Guide

Microsoft Customer

this is the latest version of security update, the 'September 2003, Cumulative Patch' update which fixes all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to protect your computer. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 9.00 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest opportunity.
How to install	Run attached file. Choose Yes on displayed dialog box
How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact Us.

Figure 2. Example of spoofed email used to spread a computer virus.

The most widespread approach that identity thieves use is to first register a misleading domain name, then erect a "phisher" website that is similar to the legitimate one, and finally send customers an email that appears to originate from the targeted company. The email entices the customer to visit the website with an offer that's too good to refuse, or by convincing them that there is a need to enter or update account information. The identity thieves who attacked Best Buy customers actually posed as the "Best Buy Fraud Department" (see Figure 1.)

Once the personal information is collected, it is sometimes used by the perpetrator, but more often it's sold or traded to other criminals who use it for credit card fraud or personal identity theft. These exchanges are commonly made in Internet chat rooms.

While financial gain is the most common reason for corporate identity theft, some attackers use the crime to further other interests. Activists, for example, sometimes use corporate identity theft to publicize a perceived wrongdoing or cast the targeted company in a negative light. Hackers may use corporate identity theft to steal passwords or spread a computer virus. This approach was evident in a recent case of corporate identity theft targeted at Microsoft (see Figure 2.)

"Phishing" scams designed to steal account information are the most common form of corporate identity theft.

```
-----Original Message-----
From: aw-confirm@ebay.com [mailto:aw-confirm@ebay.com]
Sent: Tuesday, September 16, 2003 2:53 AM
To: abc678@aol.com
Subject: Changed eBay User ID

Dear abc678@aol.com

eBay is constantly working to provide a safer and easier trading
experience for our members. In our ongoing efforts to prevent
unsolicited and possibly fraudulent email, we have decided to allow
only User IDs that do not include an email address. This policy takes
effect immediately.

Your User ID includes an email address, and must now be changed. To
avoid any interruption in your ability to trade on eBay, we have chosen
a temporary User ID for you:

New User ID: abc6781

Your password and email address on file have not been changed. You will
not receive a 'Changed ID' icon because of this change.

If you would like to change your temporary User ID, please sign in at
http://pages.ebay.com/ with your new User ID. Then use the 'Change User
ID' feature (Preferences area of My eBay) to choose your new eBay User
ID. If you have any questions, you can learn more about the 'Change
User ID' feature and how it works in our Help section.

For more information on this policy regarding User IDs, refer to 'User
ID Policy' in Help at http://pages.ebay.com/.

Regards,
EBay
---------------------------------------------------------------

Copyright © 2003 eBay Inc. All Rights Reserved.
eBay will not request personal data (password, credit card/bank
numbers) in an email.
Designated trademarks and brands are the property of their respective
owners.
eBay and the eBay logo are trademarks of eBay Inc.
```

Figure 3. Example of corporate identity theft targeted at eBay customers

Who's At Risk

The FBI has seen a steady increase in complaints involving unsolicited e-mails directing consumers to bogus banking sites.

Corporate identity thieves have targeted companies in nearly every industry, but since most identity theft is perpetrated to facilitate financial crimes, banks and other financial services companies have the greatest reason to be alarmed. In September 2003 the US Office of the Comptroller of the Currency (OCC) reported that the FBI's Internet Fraud Complaint Center (IFCC) has seen a steady increase in complaints involving unsolicited e-mails directing consumers to bogus banking sites or directly asking for personal financial information. The OCC warned banks to take all possible precautions to protect customers from a recent proliferation of Web-spoofing e-mail scams.

Companies with a significant online presence are also finding themselves the target of increasingly frequent attacks. This is because it's easier to target customers of organizations like ISPs, registrars, e-commerce merchants, and auction sites. Identity thieves can often harvest customer email addresses from online directories. Many of the major Internet companies like AOL, eBay, Amazon.com, EarthLink, Verisign, or 1-800-Flowers.com have customer bases large enough that even a random spam email attack is likely to end up in a significant number of customer email boxes (see Figure 3.) The customers of these organizations are also an attractive target because they all maintain account information online that includes the credit or debit card numbers sought by identity thieves.

Detecting and Combating Corporate Identity Theft

Each step that a corporate identity thief takes when perpetrating crime offers an opportunity for potential victims to detect the attack, sometimes before any customers are affected. What follows is a four step process that organizations can use to help detect and avert corporate identity theft attacks. The first three steps offer companies an opportunity to take action at each of the following common stages: domain registration, site construction, and sending spam email.

Step 1. Monitor Domain Registrations

Each step that a corporate identity thief takes when perpetrating their crime offers an opportunity for potential victims to detect the attack.

There are two reasons why identity thieves are registering domains. One is that spam email filters will flag hyperlinks to IP addresses, and since spam email is a favored vehicle for luring customers, identity thieves must use a registered domain name if they want to be sure their emails reach their targets. The second reason that most convincing "phisher" websites register a domain name is that it further enhances their ruse. The name will typically be similar to the legitimate site, or even include the company name in the address. Some registered domains include common typos or misspellings as a mechanism to capture unsuspecting customers who type their intended destination directly into their browsers.

The following are examples of domains registered to target eBay customers:

- customerserviceebay.com
- info-update-ebay.net
- ebayaccountinfo.co.uk
- ebay-cg1.com
- 3signin-ebay.com
- cgi4-ebaysupport.ca
- ebaysecureacount.com

If an offender uses an entirely unrelated or random domain name they will risk making customers suspicious and reduce the likelihood of a successful scam.

Because of the similarity between fraudulent and legitimate domains, businesses are afforded an opportunity to detect a threat of corporate identity theft before it ever happens. By reviewing a daily alert of newly registered domains, a company can flag suspicious domains and monitor them for illicit activity.

Best practice is to determine your course of action in advance.

If the domain name infringes on a trademark, such as those shown in the eBay example, the company can pursue the offending party for cybersquatting. If a fraud is already underway, the company can contact law enforcement, the ISP, and/or the registrar. Best practice is to determine your course of action in advance and establish relationships with the parties who can help take down sites if an attack occurs.

To facilitate the management of domain names, companies should not only monitor new registrations but also centralize the registration process and know what they already own. If they don't, it can be difficult to detect a rogue registration, particularly if a criminal provides the target company information in the registration information, making the registration appear legitimate on cursory examination.

Finally, its worthy to note that there was a time when Internet fraudsters would always use an IP address for their fake websites, saving them the time and trouble of registering a domain name. While some identity thieves still don't register domains; many of them do, paying with a stolen credit card and using bogus contact information. Unfortunately, most registrars make little effort to authenticate the identification of registrants, making it easy to provide bogus information or no information at all. Some registrars, such as GoDaddy, even offer anonymous registrations as an option.

Step 2. Monitor the Web

The next step a corporate identity thief takes before launching an attack is erecting a website. As such, monitoring the Web for the appearance of these sites is the second step in protecting yourself from corporate identity theft. While monitoring global registrations is a great proactive approach, and must be done, it can't stand on its own. This is because there are many forms of corporate identity theft that cannot be detected solely by monitoring domain names. Examples of "phisher" websites that might not be detected by monitoring domain registrations include the following:

- Sites such as those referenced earlier that can be found only by knowing the IP address. For the reasons already discussed, these are not as common as they once were, but they still exist.

Even if you find the domain, sometimes the homepage won't link to the page where the crime is being committed.

- Fraud sites whose domain names don't include any variations of the targeted company trademarks. Since there are typically more than 10,000 new registrations per day in the gTLDs alone, it makes sense to focus on those that appear to be targeting your company. Some "phisher" sites might register domains that have more generic domains. In this case they frequently use the company name in a sub-domain or somewhere else in the page's URL so that they appear legitimate. Another indication of a potential fraud site is the presence of an @ symbol anywhere in the page URL.

- Fraud web pages that are "orphan" pages which cannot be detected from a domain homepage. In other words, even if you find the domain, sometimes

the homepage won't link to the page where the crime is being committed. Oftentimes, the home page will say something like "under construction" and there will be no links that exist to a live fraudulent page, and thus there is no way to know the address or find it without a hyperlink, which is usually located in spam email.

There are a number of ways that companies can monitor the Web, some more effective than others. The following is a brief list, together with their advantages or limitations:

Implement a program that makes it easy for employees and customers to report any suspicious websites that they encounter.

- Implement a program that makes it easy for employees and customers to report any suspicious websites that they encounter. This is a good idea regardless of what other monitoring techniques are employed. Unfortunately, it means you won't learn about a corporate identity theft incident until the attack has already been launched and you risk learning about it from your customers.

- Conduct regular reviews of the search results on major search engines. The effectiveness of this approach is limited by the lack of Web-based links to fraud sites and, when links do exist, the delay before they are crawled and appear in the search engine's index. You can still uncover some "phisher" sites by monitoring search engine results, though it is not particularly effective or efficient.

- Subscribe to a service that will monitor the Web on your behalf. Outsourcing can provide the most comprehensive early detection solution, but the service will only be effective if it does not rely on commercial search engines. In addition to crawling the web, the vendor must monitor web pages reached by extracting hyperlinks from other online sources, such as spam and message boards. Timing is important so results from this "cross feed" should be reported daily or as close to real-time as possible. Ideally, the service should send you an alert as soon as an incident is detected.

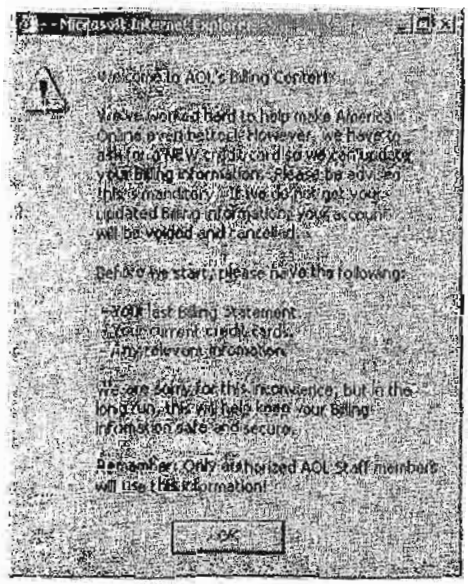


Figure 4
Fake AOL Billing Center launches a welcome notification.

Corporate identity theft websites and pages are usually carefully designed to appear identical to the genuine ones (see Figures 4 and 5.) In fact, almost all of the "phisher" sites are the result of copying exact code and images from the legitimate page. Many of the bogus sites further confuse customers by including links to a company's real pages, such as privacy statements or other disclaimers. Tracking the sources of inbound traffic to your privacy statement could uncover fraudulent sites, as could searching the Internet for hyperlinks to that page.

The meticulous detail reflected in the fraudulent sites makes it difficult to distinguish the fake from the real thing, but it also empowers the targeted company. Many fraud sites and emails are infringing on copyrights. Under the provisions of copyright laws such as the Digital Millennium Copyright Act (DMCA) and the European Union Copyright Directive (EUCD), affected businesses have a variety of tools at their disposal to take action against the offending site.

Many fraud sites and emails are infringing on copyrights, giving the legitimate owner the power to take action.

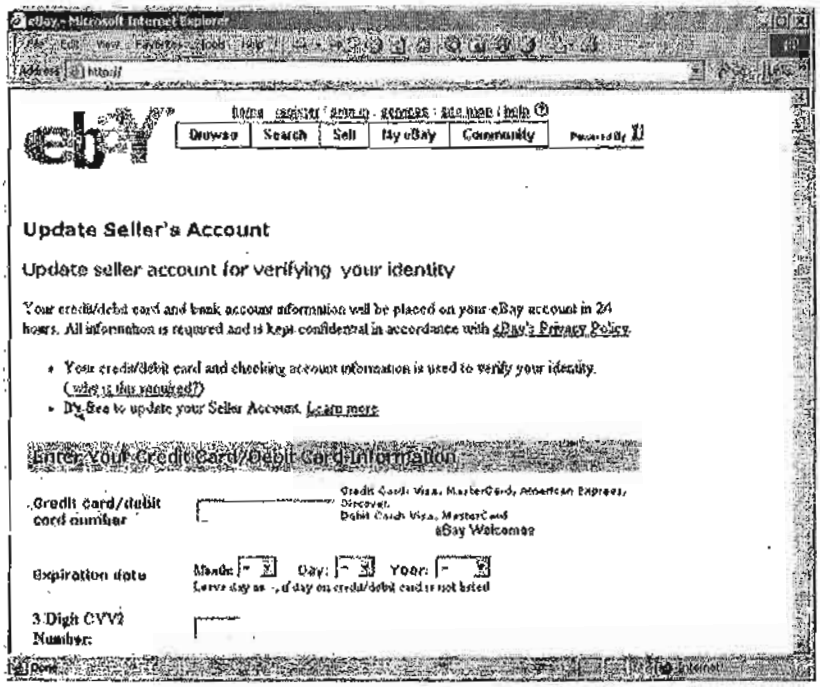


Figure 5. Fraudulent ebay website appears identical to the real one.

Step 3. Monitor spam email

There are many different mediums by which an identity thief can reach a business' customers and lure them to a "phisher" website. The five most common vehicles include the following:

Spam email is by far the most common manner by which identity thieves currently reach a business' customers.

- Hyperlinks from spam email
- Hyperlinks from the Web, Usenet, chat rooms, or other online environments
- Direct traffic through typopiracy and cybersquatting
- Advertising, adware, or paid placement

Spam email is by far the most common manner by which identity thieves currently reach a business' customers. This is because email allows the identity thief to easily reach the largest number of customers in the shortest amount of

time, at a negligible cost. Spam email can be easily altered so that it appears to have originated from a legitimate source, and can be designed to be practically indistinguishable from the real thing.

The tricks employed are sometimes very clever and although many companies and organizations have tried to educate consumers on how to detect a fraudulent email, even Internet experts can sometimes find it difficult. For this reason, when companies are educating consumers to be on alert, they are advised to consider the following:

The best approach is for consumers to simply avoid clicking on any links in unsolicited email.

- Never contact your customers via email for any reason that would require them to share personal information, or even to log into your site by clicking through a link in the email. Repeatedly remind your customers of this policy and reinforce its importance.

- Tell your customers to NEVER click on links in email. Customers should instead directly type or bookmark trusted Internet destinations. If an email arrives asking to update account information, the customer should type the destination website directly into their browser rather than click the link provided.

While raising awareness of the issue is important, you need to ensure that a false sense of security is not created among customers who feel they're armed with all the knowledge necessary to spot a fake. The truth is that fraudsters are constantly rolling out new tricks, some of which are very complicated to decipher, even for the savviest of surfers. The best approach is for consumers to simply avoid clicking on any links in unsolicited email, and travel to their desired destination directly, or through a trusted source such as a reputable Internet portal.

Identity thieves also believe that most companies do not know how to monitor spam email nor detect when an attack is occurring. This is sometimes true, though there are two ways a company can tackle this challenge:

The first way to monitor spam is to engage the help of company stakeholders to monitor for abuse. As with monitoring the Web, employees, suppliers, distributors, and even customers or investors can help a company monitor for spam-based corporate identity attacks. Almost everyone has personal email accounts and receives spam daily, oftentimes in high volumes. If a large company can educate their employees, for example, and provide incentives and an easy way to report suspicious email, they can effectively monitor tens or even hundreds of thousands of spam emails per day. Disadvantages of the stakeholder monitoring approach include the following:

- It is by definition a reactive approach, meaning that you don't learn about an incident until an attack has been launched.
- Implementing and managing the program can be an involved, time-consuming process.
- Asking your employees to monitor spam could affect productivity.

The second effective way to monitor spam is to outsource the function to a vendor. Cyveillance, for example, monitors and analyzes hundreds of thousands of spam emails daily for their clients. Cyveillance technology scans each email and crawls all links to find incidents of corporate identity theft. It also includes

an alarm function that can notify a client of an attack-24x7x365, maximizing your ability to take action before damage occurs.

Step 4. Get Involved

Recognizing the broader implications of corporate identity theft, companies and organizations around the world have begun to work together to address the issue. Only through high levels of cooperation will the public and private sectors be able to successfully combat the problem. Industry coalitions and working groups have begun to emerge that can serve as resources for affected companies.

On September 2, 2003 the Information Technology Association of America (ITAA) announced that a group of leading financial services, information technology and electronic commerce companies and organizations had formed an industry coalition to fight online identity theft. The Coalition on Online Identity Theft will work to address four primary areas:

- Expand public education campaigns against online identity theft to protect consumers;
- Help promote technology and self-help approaches for preventing and dealing with online identity theft;
- Document and share non-personal information about emerging online fraudulent activity to stay ahead of criminals and new forms of online fraud;
- Work with government to cultivate an environment that protects consumers and businesses, and ensures effective enforcement and criminal penalties against cyber thieves.

According to ITAA President Harris N. Miller, the Coalition is reaching out to other companies and organizations interested in seeking educational, legal and technical solutions to protect consumers and companies from online fraud and safeguard the future of e-business. "Ultimately, the solution is a shared responsibility among industry, government and consumers to advance education and awareness, stronger penalties, cooperation within industry and law enforcement, and work together to prevent the spread of this problem into e-commerce," Miller said.

In another recent development, Bank One announced that they are partnering with the US Postal Inspection Service and other government entities for a new identity theft public awareness program called "Operation: Identity Crisis," a prevention campaign to raise awareness among business and consumers. "Identity theft is significant, serious and a growing concern," said Chris Conrad, senior vice president of fraud management for Bank One. "It's something that consumers and businesses need to get educated about..."

Conclusions

Each step in the process used to perpetrate identity theft represents an opportunity for the targeted company to detect an emerging threat and take action.

Corporate identity theft is a growing problem online that can affect almost any company and can cause serious damage. While there are a wide variety of means by which the crime can be committed, common patterns have emerged. Perpetrators will typically register a domain name, construct a "phisher" website, then send a spam email designed to lure customers under false pretences for the purpose of stealing their personal information.

Each step in the process used to perpetrate identity theft represents an opportunity for the targeted company to detect an emerging threat and take action. By monitoring suspicious domain registrations and websites, a company can sometimes learn of an imminent attack before any customers are affected. By working collaboratively and extending monitoring efforts to spam email, a company can take action to further limit their exposure and protect other customers from being victimized.

About Cyveillance

Cyveillance, the leading provider of 100% Relevant eBusiness Intelligence™, provides Global 2000 organizations with high-impact, actionable intelligence drawn from—and delivered securely over—the Internet. The company's product offerings include CySecurity, an early warning system for businesses to proactively identify risk; CyMarketplace, a service that dramatically improves the performance of online distribution channels; and CyWebWatch, a high ROI solution enabling clients to pinpoint and eliminate online intellectual property abuse that is impacting their bottom line and reputation. The company lists over 20 of the Fortune 50 as customers.

Cyveillance is a founding member of the Coalition on Online Identity Theft, an organization formed by Microsoft Corp., RSA Security Inc., eBay Inc., Verisign, Amazon.com, McAfee Security, and several other leading companies to fight online identity theft.

For more information, please call 888.243.0097 or visit www.cyveillance.com.

About the Author

Brian H. Murray is vice president of client services at Cyveillance, Inc. and author of the book *Defending the Brand: Aggressive Strategies for Protecting Your Brand in the Online Arena*. Mr. Murray has appeared as an expert on CNNfn, TechTV, CNET Radio, and CBS MarketWatch, and his work has been reported globally by news media such as USA Today, The New York Times, The Wall Street Journal, Sky News, Investor's Business Daily, the BBC, and The Financial Times. In 2002 and 2003 Mr. Murray was appointed as an expert advisor to the Virginia General Assembly's Joint Commission on Technology and Science. In 2003 he was selected to be a founding member of the American Management Association's Homeland Security Council.

Cyveillance
Binding your business on the Net

1555 Wilson Boulevard
Suite 404
Arlington, VA 22209-2405

Tel: 703.351.1000
Fax: 703.312.0536
www.cyveillance.com

RIF