2021 Higher Education Virtual Conference

February 9, 2021

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Disclaimer

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Higher Education Virtual Conference

Legislative and regulatory landscape:
What could lie ahead for colleges and universities

-Tom Netting, TEN Government Strategies

TUESDAY, FEBRUARY 9, 2021

Consolidated Appropriations Act of 2021

- Labor, Health and Human Services, Education and Related Agencies Appropriations

- Coronavirus Response and Relief Supplemental Appropriations Act of 2021

- FAFSA Simplification

Consolidated Appropriations Act of 2021

- **Labor, Health and Human Services, Education and Related Agencies Appropriations**
  - Increase in Federal Pell Grant ($22 Billion)

    $150 Increase in the Maximum Federal Pell Grant ($6,495)
  - Increases in Other Federal Grant Assistance Programs (TRIO, SEOG, & FWS)
  - FAFSA Simplification
  - Ability to Benefit
  - Postsecondary Transfer Articulation Agreements

Consolidated Appropriations Act of 2021

- **Coronavirus Response and Relief Supplemental Appropriations Act of 2021**
  - Additional Education Stabilization Funds ($22,6 Billion)
    - 89% ($20,200,451,040) to each institution of higher education as defined in section 101 or section 102(c) of the HEA to prevent, prepare for, and respond to coronavirus;
    - 7.5% ($1,702,285,200) for additional awards under parts A and B of title III, parts A and B of title V, and subpart 4 of part A of title VII of the HEA to address needs directly related to coronavirus, that shall be in addition to awards made in subsection (a)(1); and
    - 3% ($680,914,080) to institutions of higher education as defined in section 102(b) of the HEA.

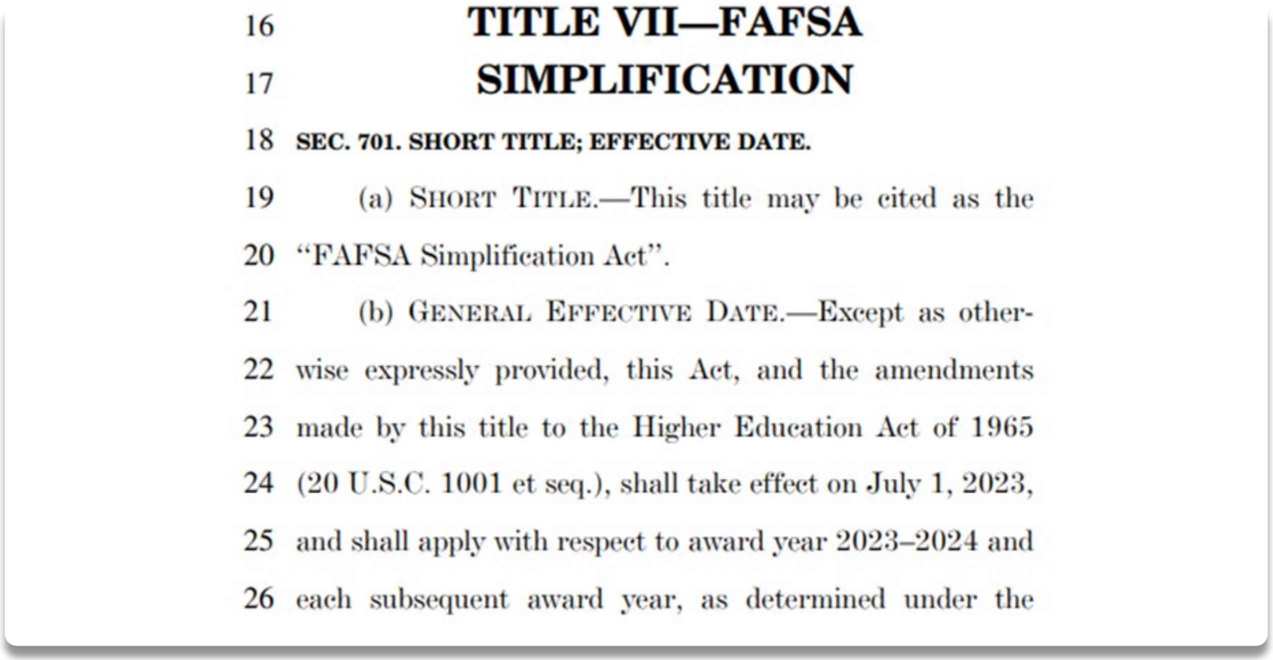
Consolidated Appropriations Act of 2021

- **Coronavirus Response and Relief Supplemental Appropriations Act of 2021**
  - Additional Education Stabilization Funds ($22 Billion)
    - 89% ($20,200,451,040) to each institution of higher education as defined in section 101 or section 102(c) of the HEA to prevent, prepare for, and respond to coronavirus;
    - 7.5% ($1,702,285,200) for additional awards under parts A and B of title III, parts A and B of title V, and subpart 4 of part A of title VII of the HEA to address needs directly related to coronavirus, that shall be in addition to awards made in subsection (a)(1); and
    - 3% ($680,914,080) to institutions of higher education as defined in section 102(b) of the HEA.

Consolidated Appropriations Act of 2021

FAFSA Simplification

- Needs Analysis
- Student Aid Index
- Cost of Attendance
- SFA Administrator Discretion
- Student Eligibility
- Second Chance Pell



TITLE VII—FAFSA SIMPLIFICATION

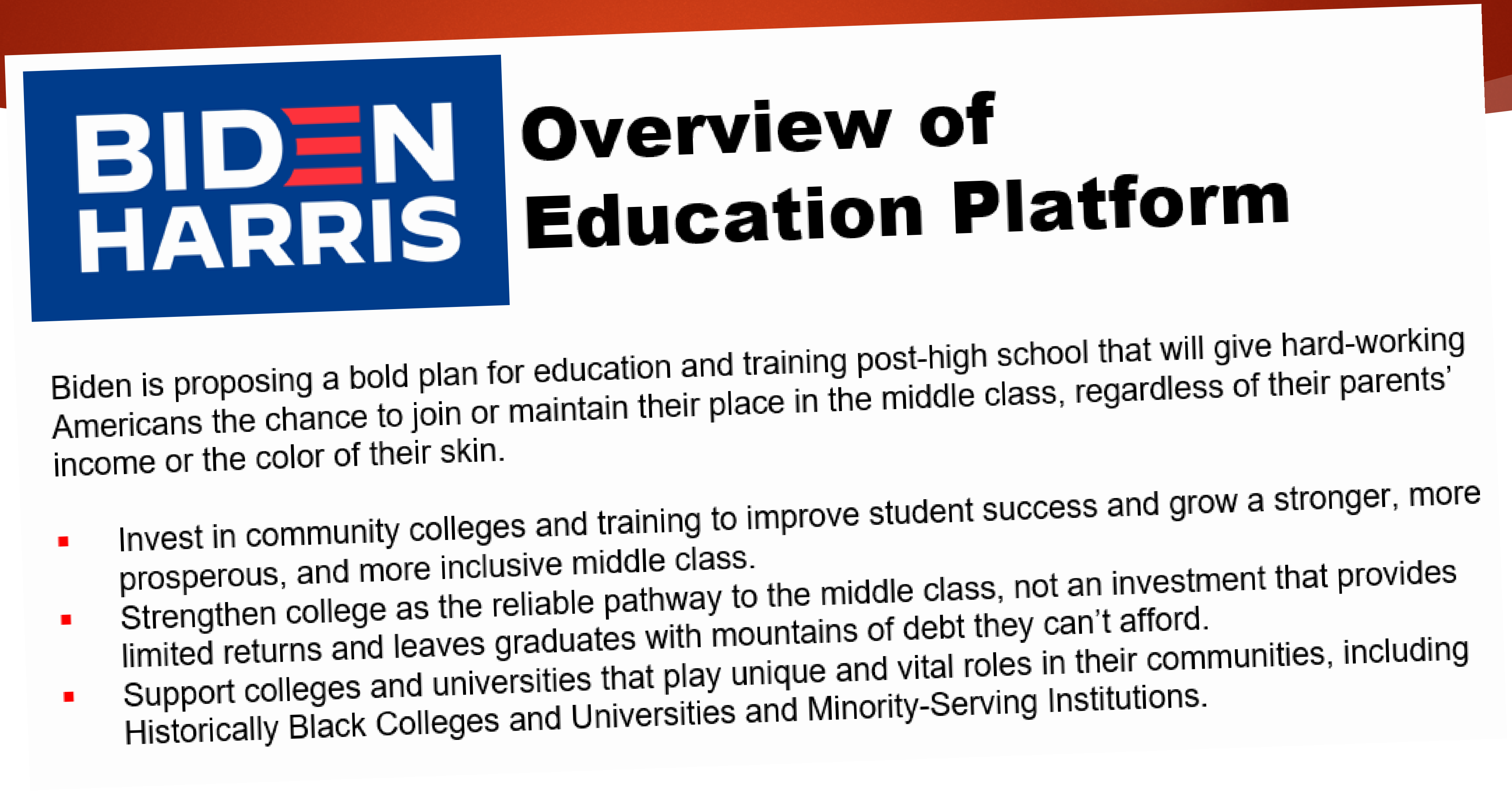
SEC. 701. SHORT TITLE; EFFECTIVE DATE.

(a) SHORT TITLE.—This title may be cited as the "FAFSA Simplification Act".

(b) GENERAL EFFECTIVE DATE.—Except as otherwise expressly provided, this Act, and the amendments made by this title to the Higher Education Act of 1965 (20 U.S.C. 1001 et seq.), shall take effect on July 1, 2023, and shall apply with respect to award year 2023–2024 and each subsequent award year, as determined under the

BIDEN
HARRIS

Higher Education Platform

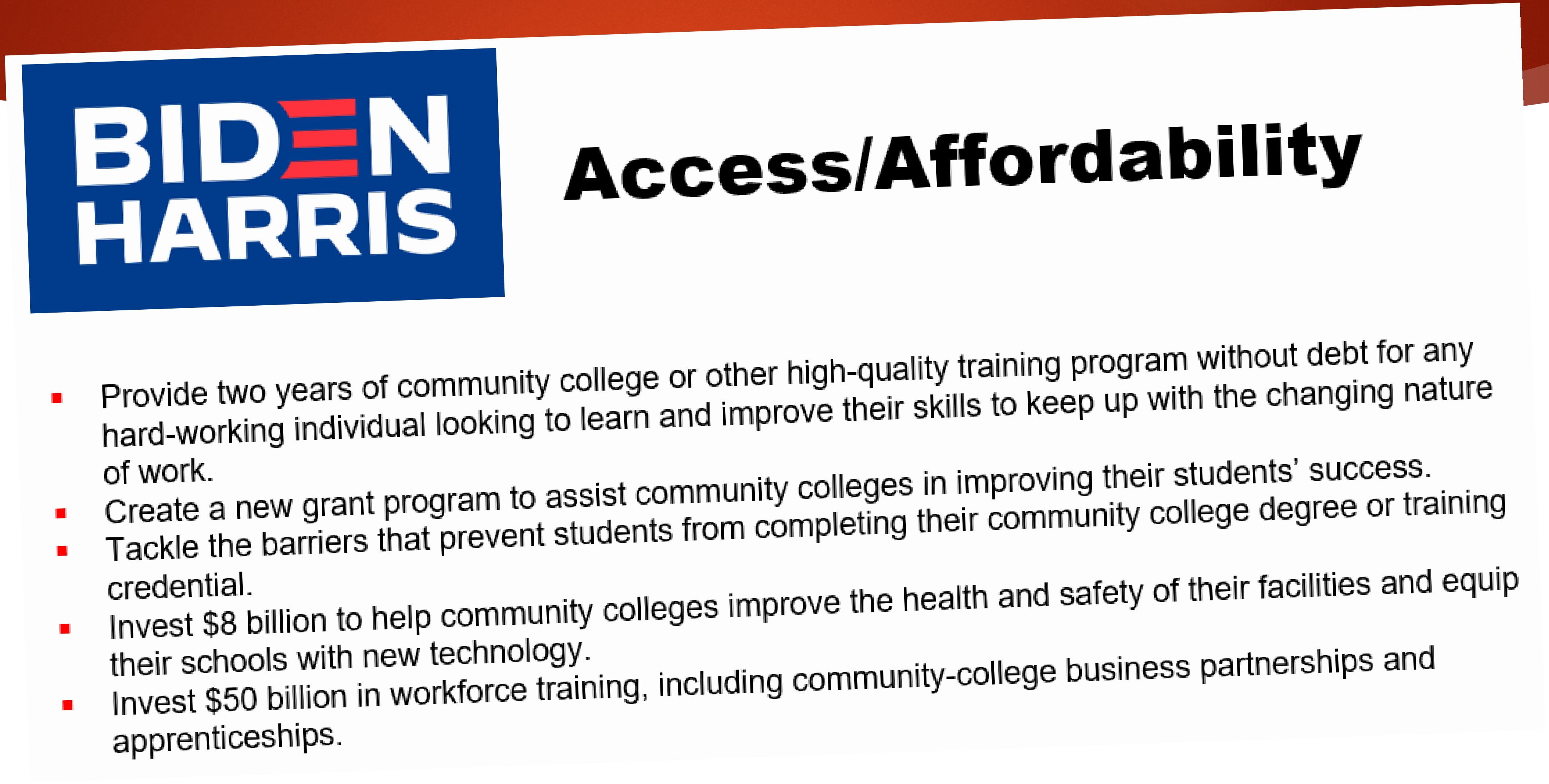


BIDEN HARRIS

Overview of Education Platform

Biden is proposing a bold plan for education and training post-high school that will give hard-working Americans the chance to join or maintain their place in the middle class, regardless of their parents' income or the color of their skin.

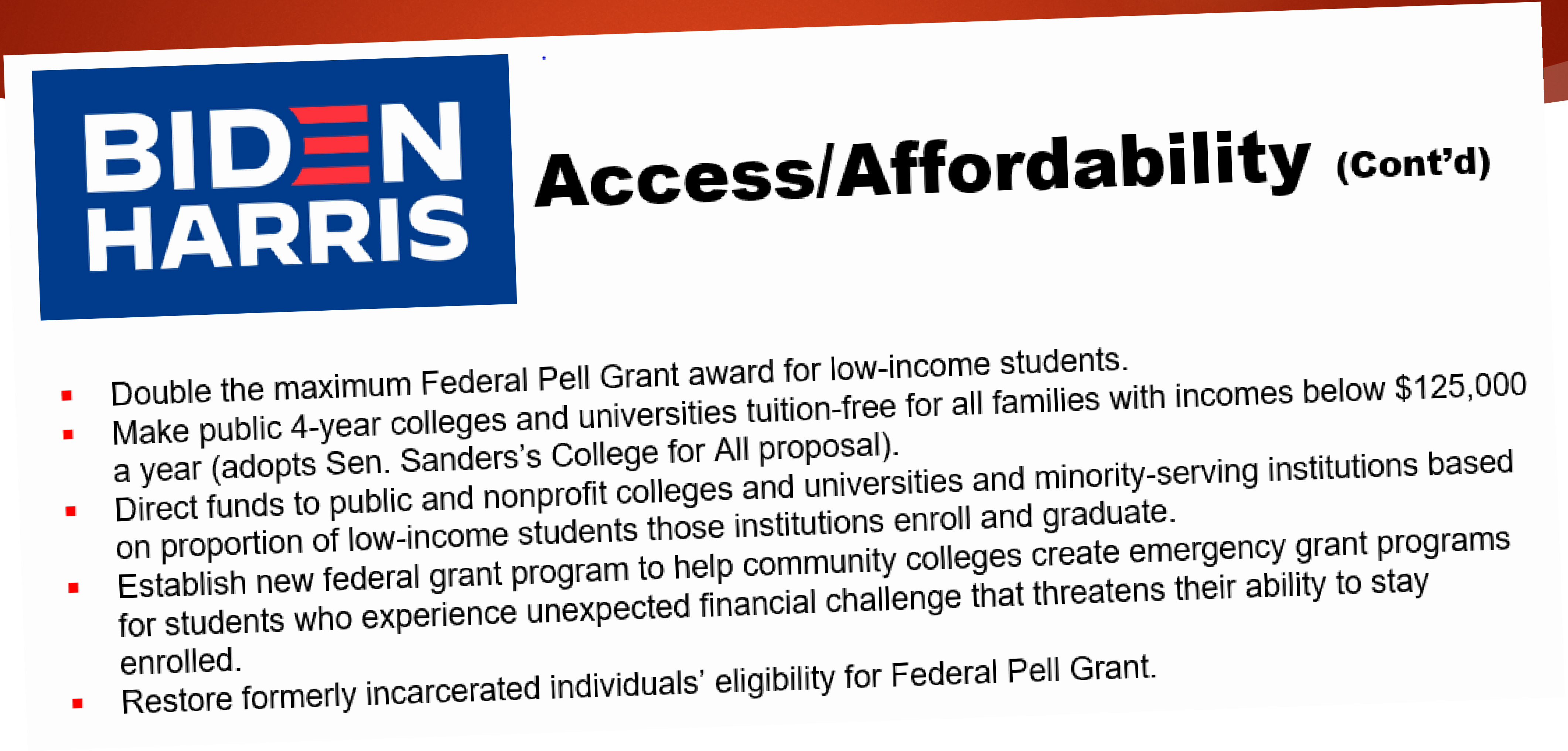
- Invest in community colleges and training to improve student success and grow a stronger, more prosperous, and more inclusive middle class.
- Strengthen college as the reliable pathway to the middle class, not an investment that provides limited returns and leaves graduates with mountains of debt they can't afford.
- Support colleges and universities that play unique and vital roles in their communities, including Historically Black Colleges and Universities and Minority-Serving Institutions.



BIDEN HARRIS

Access/Affordability

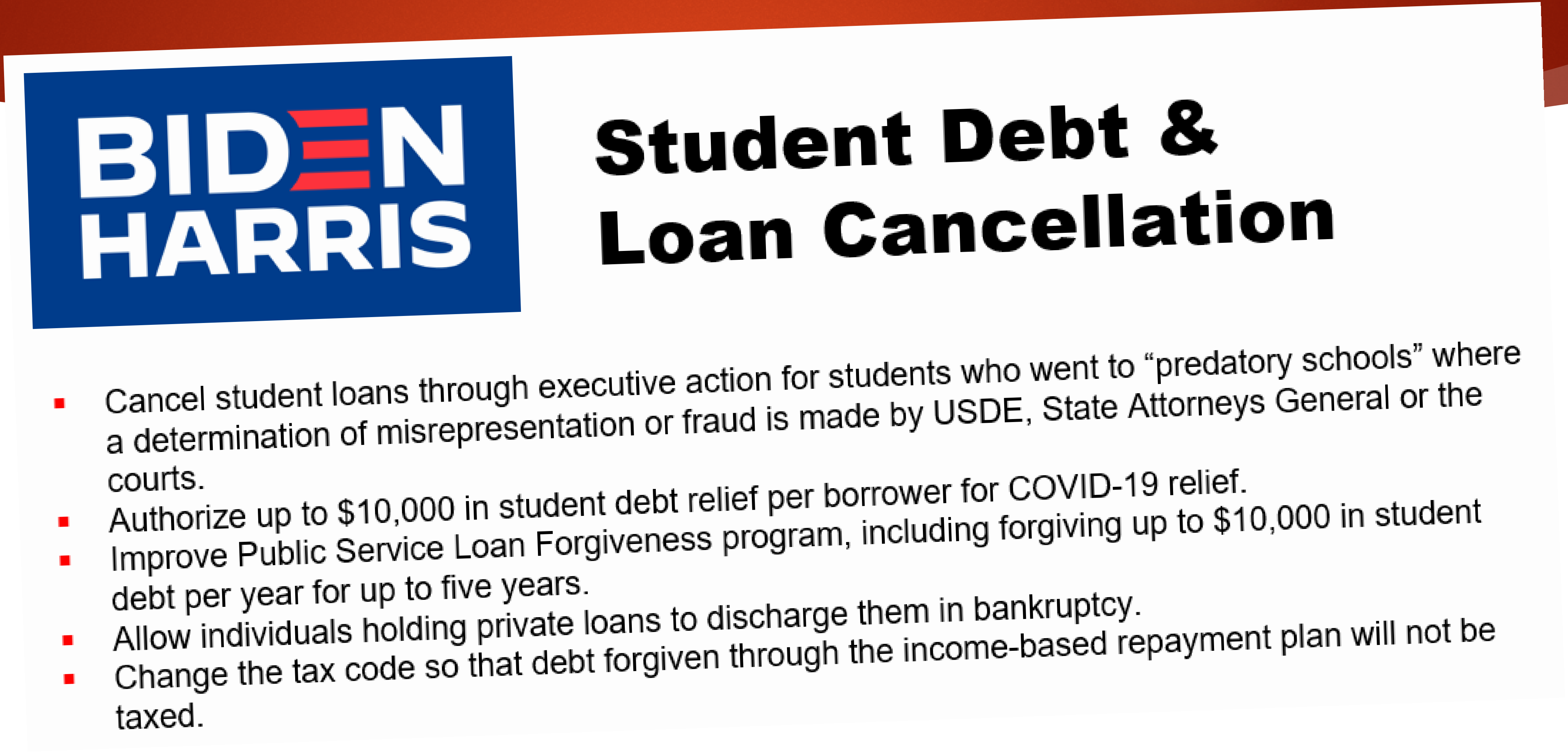
- Provide two years of community college or other high-quality training program without debt for any hard-working individual looking to learn and improve their skills to keep up with the changing nature of work.
- Create a new grant program to assist community colleges in improving their students' success.
- Tackle the barriers that prevent students from completing their community college degree or training credential.
- Invest $8 billion to help community colleges improve the health and safety of their facilities and equip their schools with new technology.
- Invest $50 billion in workforce training, including community-college business partnerships and apprenticeships.



BIDEN HARRIS

Access/Affordability (Cont'd)

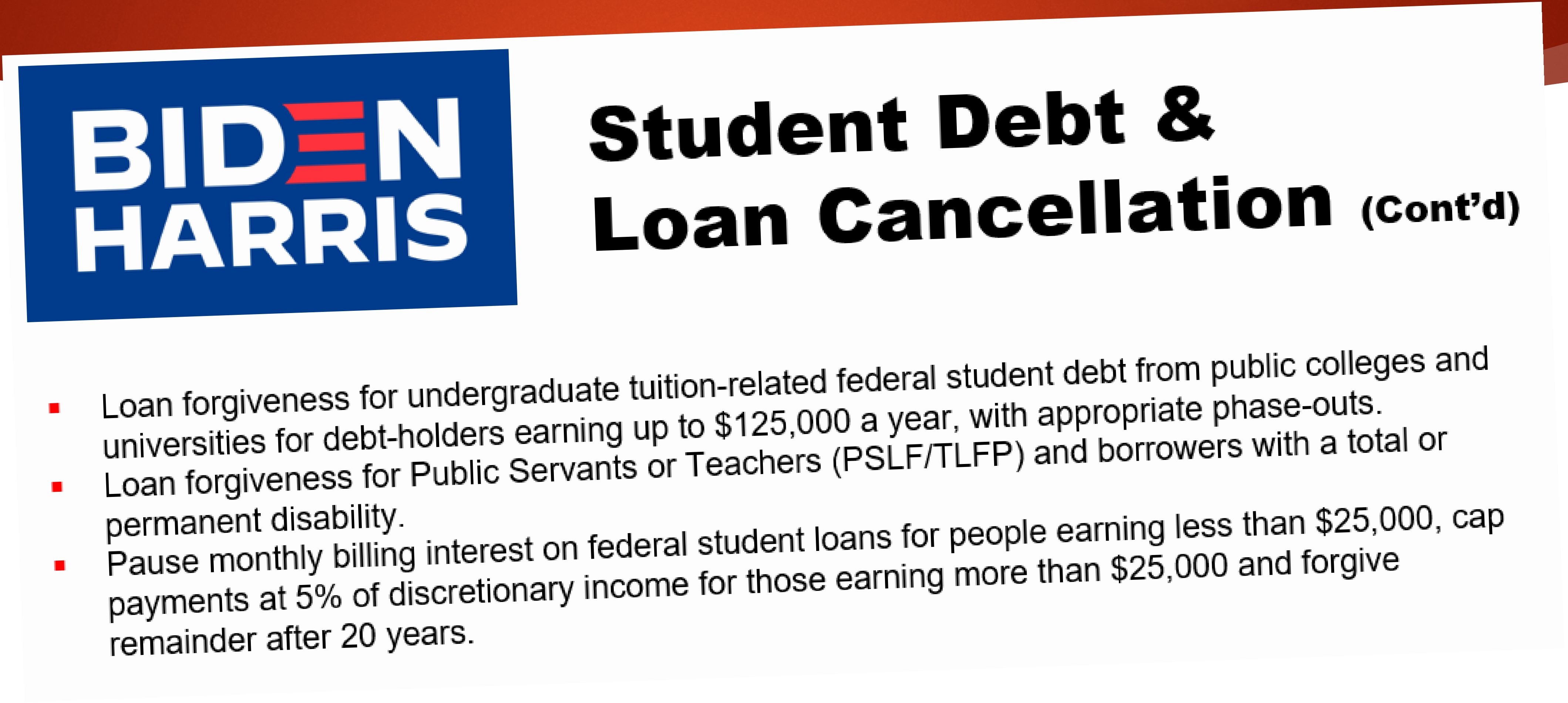
- Double the maximum Federal Pell Grant award for low-income students.
- Make public 4-year colleges and universities tuition-free for all families with incomes below $125,000 a year (adopts Sen. Sanders's College for All proposal).
- Direct funds to public and nonprofit colleges and universities and minority-serving institutions based on proportion of low-income students those institutions enroll and graduate.
- Establish new federal grant program to help community colleges create emergency grant programs for students who experience unexpected financial challenge that threatens their ability to stay enrolled.
- Restore formerly incarcerated individuals' eligibility for Federal Pell Grant.



BIDEN HARRIS

Student Debt & Loan Cancellation

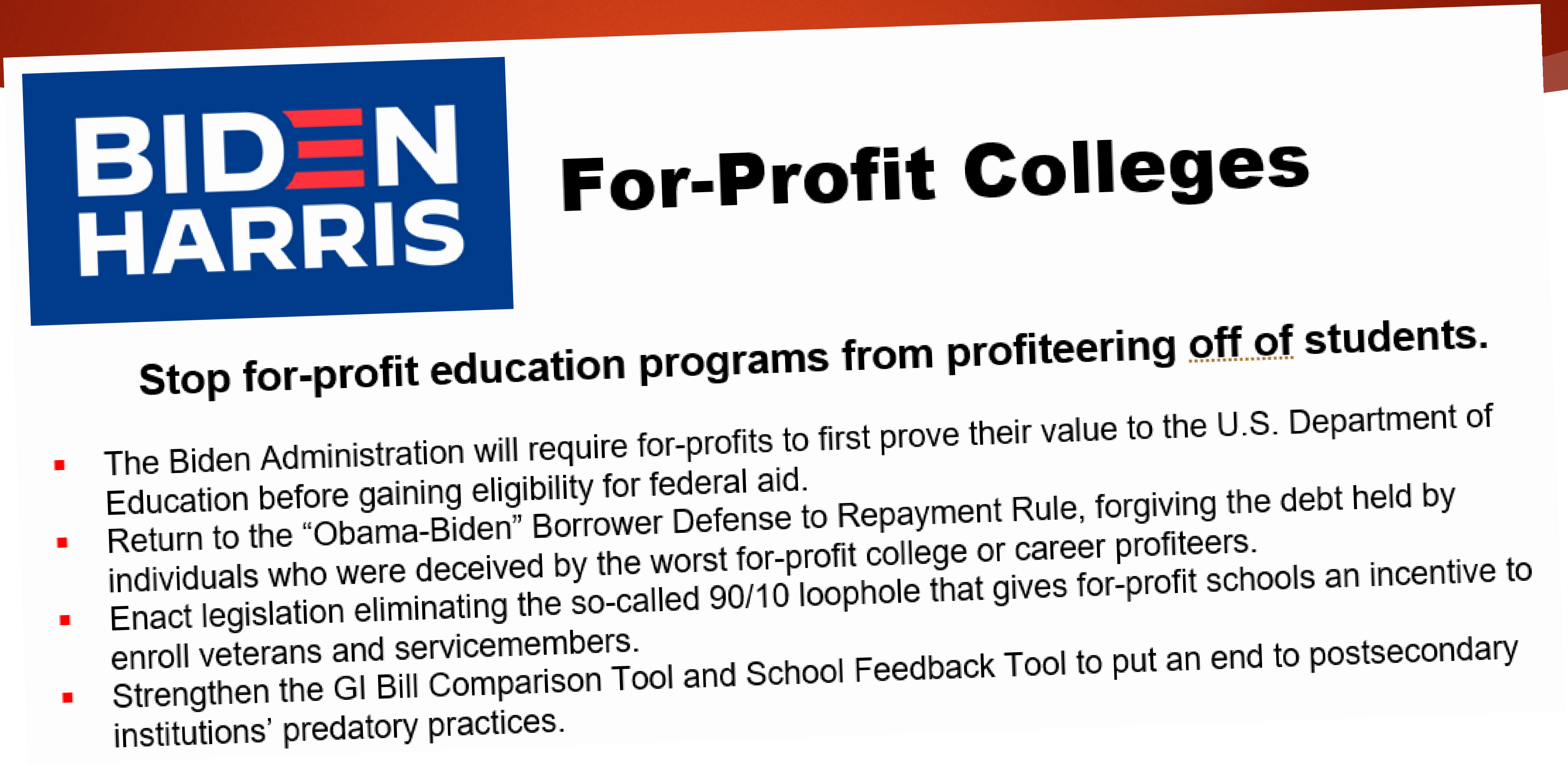
- Cancel student loans through executive action for students who went to "predatory schools" where a determination of misrepresentation or fraud is made by USDE, State Attorneys General or the courts.
- Authorize up to $10,000 in student debt relief per borrower for COVID-19 relief.
- Improve Public Service Loan Forgiveness program, including forgiving up to $10,000 in student debt per year for up to five years.
- Allow individuals holding private loans to discharge them in bankruptcy.
- Change the tax code so that debt forgiven through the income-based repayment plan will not be taxed.



BIDEN HARRIS

Student Debt & Loan Cancellation (Cont'd)

- Loan forgiveness for undergraduate tuition-related federal student debt from public colleges and universities for debt-holders earning up to $125,000 a year, with appropriate phase-outs.
- Loan forgiveness for Public Servants or Teachers (PSLF/TLFP) and borrowers with a total or permanent disability.
- Pause monthly billing interest on federal student loans for people earning less than $25,000, cap payments at 5% of discretionary income for those earning more than $25,000 and forgive remainder after 20 years.

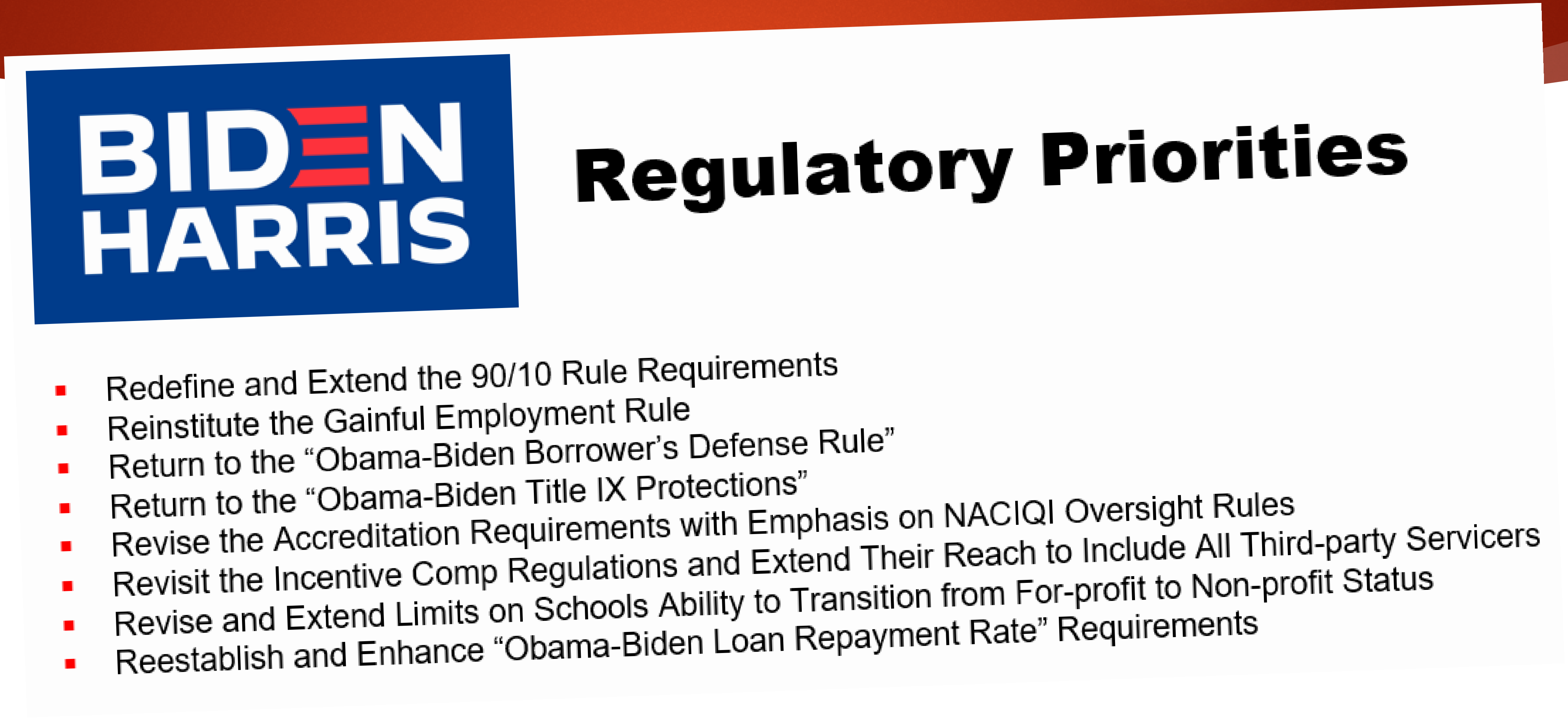


BIDEN HARRIS

For-Profit Colleges

Stop for-profit education programs from profiteering off of students.

- The Biden Administration will require for-profits to first prove their value to the U.S. Department of Education before gaining eligibility for federal aid.
- Return to the "Obama-Biden" Borrower Defense to Repayment Rule, forgiving the debt held by individuals who were deceived by the worst for-profit college or career profiteers.
- Enact legislation eliminating the so-called 90/10 loophole that gives for-profit schools an incentive to enroll veterans and servicemembers.
- Strengthen the GI Bill Comparison Tool and School Feedback Tool to put an end to postsecondary institutions' predatory practices.



BIDEN HARRIS

Regulatory Priorities

- Redefine and Extend the 90/10 Rule Requirements
- Reinstitute the Gainful Employment Rule
- Return to the “Obama-Biden Borrower’s Defense Rule”
- Return to the “Obama-Biden Title IX Protections”
- Revise the Accreditation Requirements with Emphasis on NACIQI Oversight Rules
- Revisit the Incentive Comp Regulations and Extend Their Reach to Include All Third-party Servicers
- Revise and Extend Limits on Schools Ability to Transition from For-profit to Non-profit Status
- Reestablish and Enhance “Obama-Biden Loan Repayment Rate” Requirements

BIDEN HARRIS

Proprietary Oversight 2.0

- Reestablishment of the Interagency Task Force Responsible for For-profit Oversight
- Reexamination of ACICS Recognition by National Advisory Committee on Institutional Quality and Integrity
- Repeal of New Borrower Defense to Repayment Assessment Process and Return to Obama-Biden Era Process
- Scrutiny of Use of Higher Education Emergency Relief Funds*

BREAKING
NEWS

Executive Orders

Executive Orders

Inauguration Day – January 20, 2021

Extends the existing pause on student loan payments and interest for Americans with federal student loans until at least September 30, 2021

January 21, 2021

Directs the Department of Education and HHS to provide guidance for safely reopening and operating schools, childcare providers and institutions of higher education

Executive Orders

Yet to Come?

Halt on further implementation of Title IX regulations

Inclusion of DACA Students as eligible recipients of Higher Education Emergency Relief Fund grants

Write-off of portions of existing student loan debt ($10-50K)

117th Congress

$1.9 Trillion Economic Stimulus

Omnibus Budget Reconciliation

Reauthorization of HEA

Sustainable Performance Management in Higher Education

A Conversation with Employee Performance Expert Christopher D. Lee, Ph.D.

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Disclaimer

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Learning Objectives

After this session, you'll be able to:

- Discuss 21st Century management concepts
- Describe the value of the *Performance Conversations* approach in comparison to traditional appraisal methods
- Determine whether performance conversations are a fit for your institution
- Describe how the approach can work well with an increasingly dispersed workforce

Our Higher Ed Guest
Christopher D. Lee, Ph.D.

HR SUPERSTAR

Practitioner – 25 years as a CHRO

Researcher – 15 years on performance topics

Author – 4 books

Consultant – for 75 organizations world-wide

Lecturer – @ Top 25 college

Question Writer – for PHR/SPHR exams

www.PerformanceConversations.com

Your Humble Interviewer

Sarah Conroy, SHRM-SCP, SPHR, CEBS

Higher Education Consultant

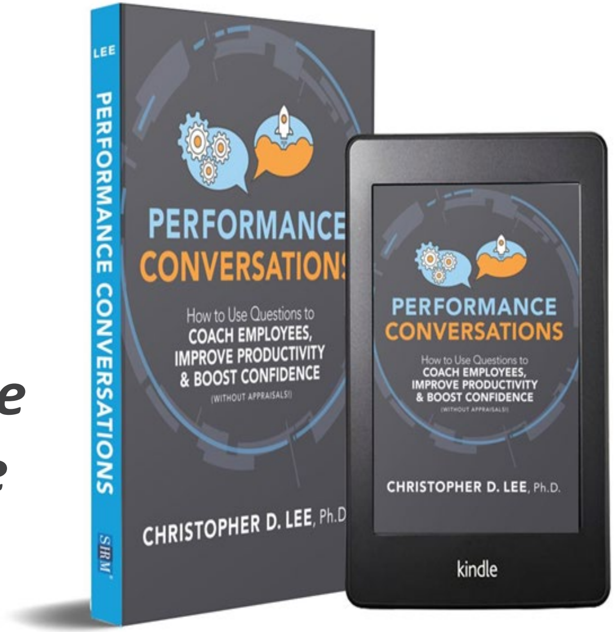
CLA Human Resources Consulting and Outsourcing

Our Conversation

Successful employee performance improvement with focus on Chris' most recent book and companion method

Performance Conversations – How to Use Questions to Coach Employees, Improve Productivity & Boost Confidence

www.performanceconversations.com



How To Learn More

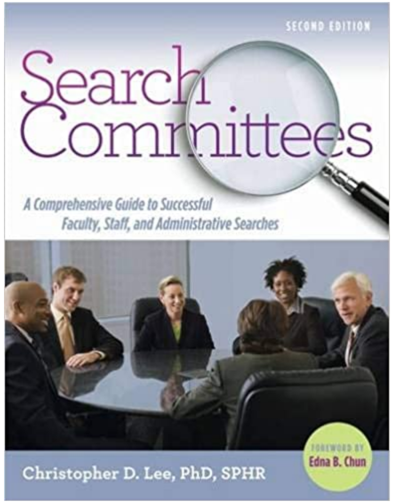
Performance CONVERSATIONS®

visit

www.performanceconversations.com

For online courses, book orders, workshops and speeches

Other Works By Dr. Lee



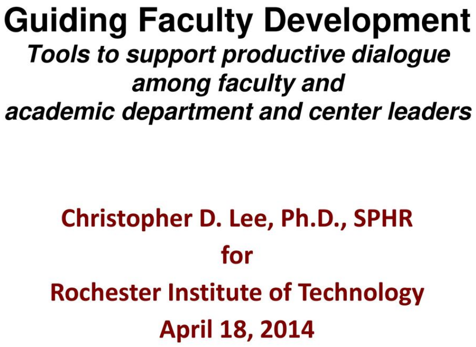
SECOND EDITION

Search Committees

A Comprehensive Guide to Successful Faculty, Staff, and Administrative Searches

FOREWORD BY Edna B. Chun

Christopher D. Lee, PhD, SPHR



Guiding Faculty Development

Tools to support productive dialogue among faculty and academic department and center leaders

Christopher D. Lee, Ph.D., SPHR

for

Rochester Institute of Technology

April 18, 2014

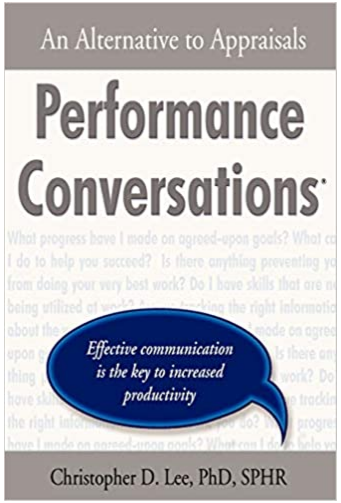
HigherEdJobs®

Aspire Higher®

How to Launch A Successful Job Search Campaign

Christopher D. Lee, Ph.D., SPHR

SearchCommittees.com



An Alternative to Appraisals

Performance Conversations®

Effective communication is the key to increased productivity

Christopher D. Lee, PhD, SPHR

Contact Information

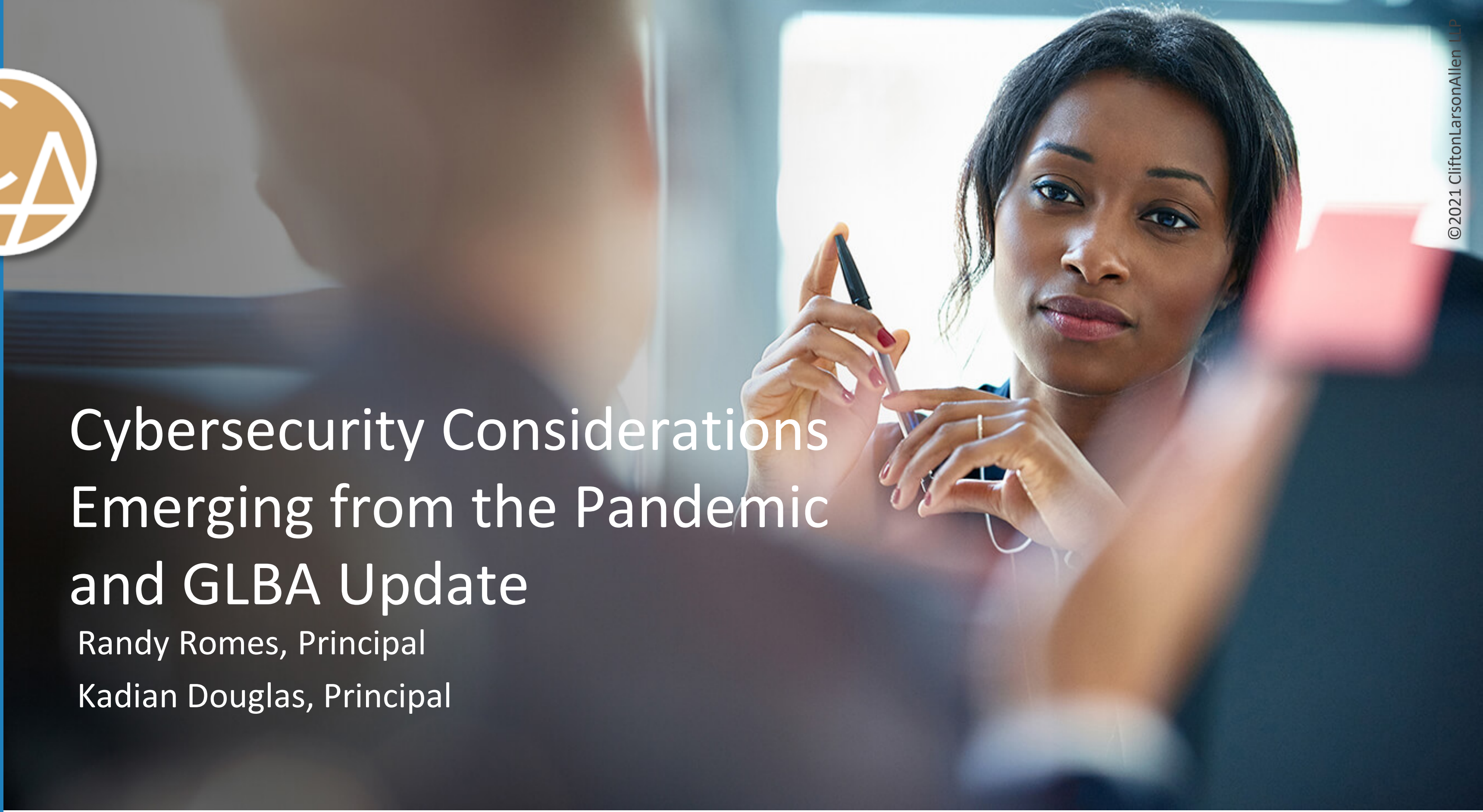
How to reach Chris

chris@performanceconversations.com

Christopher D. Lee | LinkedIn

How to reach CLA HRCO Higher Ed Team

sarah.conroy@claconnect.com



Cybersecurity Considerations Emerging from the Pandemic and GLBA Update

Randy Romes, Principal

Kadian Douglas, Principal

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Disclaimer

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user’s specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Learning Objectives

- Recognize risks relating to remote access applications and security of devices and home networks
- Review the importance of updating risk assessments and policies including vendor management, business continuity plan and incident response policies
- Revisit an example of a recent major attack and the potential impact on higher education institutions

GLBA Update

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Gramm-Leach-Bliley Act

- **Three laws covered under the Gramm–Leach–Bliley Act**
  - Pretexting Rule
    - ◊ Access to information under false pretense
    - ◊ Addressed under the Red Flags rule
  - Privacy Rule
    - ◊ Protection of and security of nonpublic information
    - ◊ In compliant once IHE is following the Family Educational Rights and Privacy Act (FERPA) regulations
  - Safeguarding Rule
    - ◊ Addresses information security policies, risk assessments and controls in place to address the risks identified

Safeguards Rule Update

- **Safeguards Rule –**
  - The Rule was issued by the Federal Trade Commission (FTC) in 2002 with industry requirement in May 2003
  - In 2015, the Department of Education included the GLBA safeguards rule compliance in its Title IV Program Participation Agreement
  - In 2019 the DOE included a portion of the GLBA safeguards rule as part of the compliance supplement single audit for student financial aid testing

Safeguards Rule Requirement

- **Safeguards Rule –**
  - Section 314.4 of the Rule noted the following:
    1. Designating an individual to coordinate your information security program
    2. Identify internal and external risk to customers' information security, information confidentiality and, integrity
    3. Design and implement information to control the risks identified during the risk assessment and regularly test the controls
    4. Oversee service providers
    5. Evaluate and update information security program based on testing and monitoring procedures

Federal Trade Commission Proposed GLBA Update

- **Potential Updates include**
  - Information security program based on risk assessment
  - Chief Information Security Officer
  - Board reporting by the person in charge of the program
  - Incident Response Plan

Federal Trade Commission Proposed GLBA Update

- **Potential Updates include**
  - Employee training
  - Detailed information security measures
  - Ongoing monitoring & testing of key controls
  - Oversight of service providers

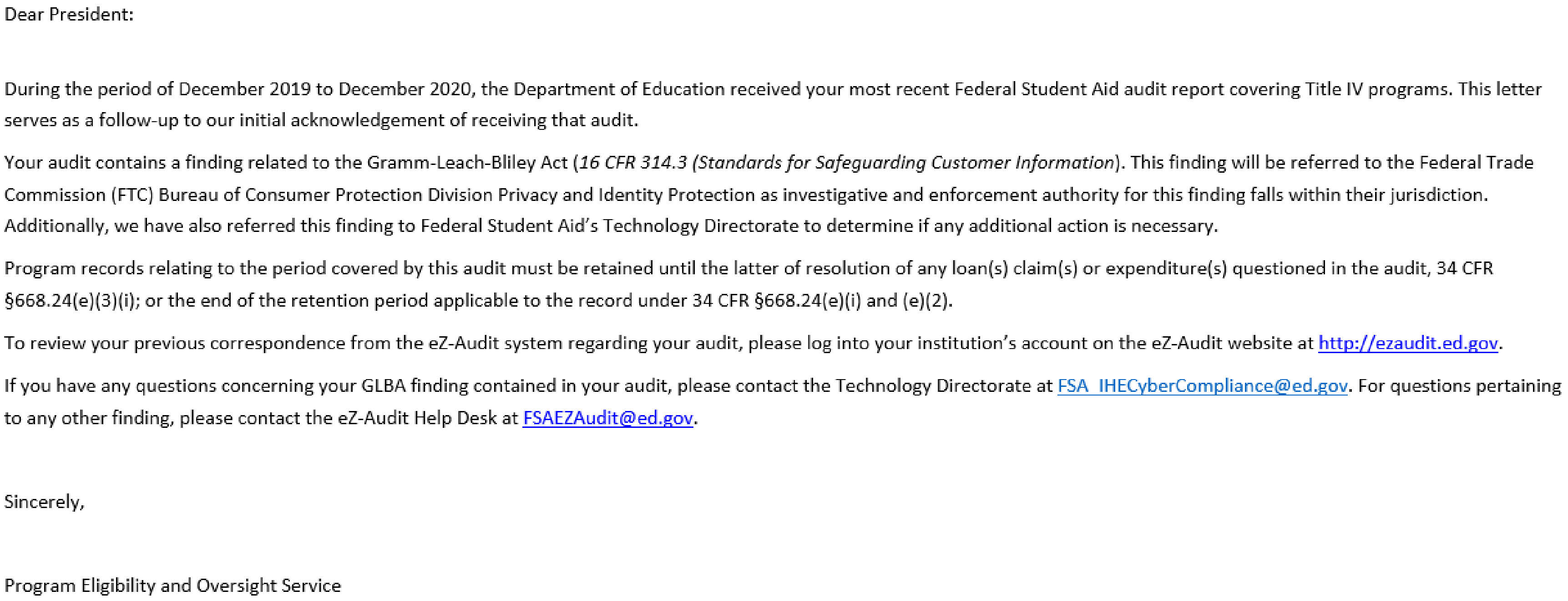
Federal Trade Commission Proposed GLBA Update

- **Potential Updates include**
  - Two additional specific requirements
    - Encryption
    - Multifactor authentication

Federal Trade Commission Proposed GLBA Update

- **Potential Updates to the Information Security Program**
    - ◊ Address access control
    - ◊ Inventory of information
    - ◊ Audit/logging
    - ◊ Disposal of information
    - ◊ Change management
    - ◊ Monitor those authorized to use the data
    - ◊ Secure development practices

DOE Communication to the FTC



Dear President:

During the period of December 2019 to December 2020, the Department of Education received your most recent Federal Student Aid audit report covering Title IV programs. This letter serves as a follow-up to our initial acknowledgement of receiving that audit.

Your audit contains a finding related to the Gramm-Leach-Bliley Act (*16 CFR 314.3 (Standards for Safeguarding Customer Information*). This finding will be referred to the Federal Trade Commission (FTC) Bureau of Consumer Protection Division Privacy and Identity Protection as investigative and enforcement authority for this finding falls within their jurisdiction. Additionally, we have also referred this finding to Federal Student Aid's Technology Directorate to determine if any additional action is necessary.

Program records relating to the period covered by this audit must be retained until the latter of resolution of any loan(s) claim(s) or expenditure(s) questioned in the audit, 34 CFR §668.24(e)(3)(i); or the end of the retention period applicable to the record under 34 CFR §668.24(e)(i) and (e)(2).

To review your previous correspondence from the eZ-Audit system regarding your audit, please log into your institution's account on the eZ-Audit website at http://ezaudit.ed.gov.

If you have any questions concerning your GLBA finding contained in your audit, please contact the Technology Directorate at FSA_IHECyberCompliance@ed.gov. For questions pertaining to any other finding, please contact the eZ-Audit Help Desk at FSAEZAudit@ed.gov.

Sincerely,

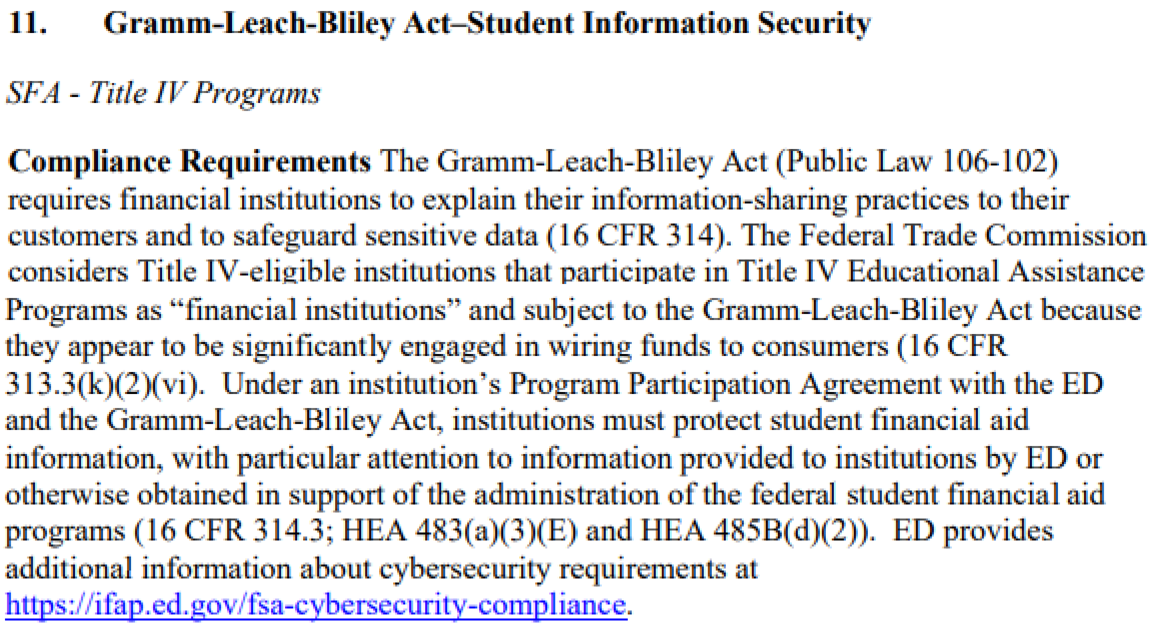
Program Eligibility and Oversight Service

Steps in Preparing for 2021 Audit

- **Follow-up on recommendations from the 2019 and 2020 audit**
- **Prepare for third party oversight to be included in future audit**
- **Be in communication with your auditor today**
- **Complete the necessary assessments prior to yearend**
- **Review prior compliance supplement**

Steps in Preparing for 2021 Audit

- **Review prior compliance supplement**



11. Gramm-Leach-Bliley Act–Student Information Security

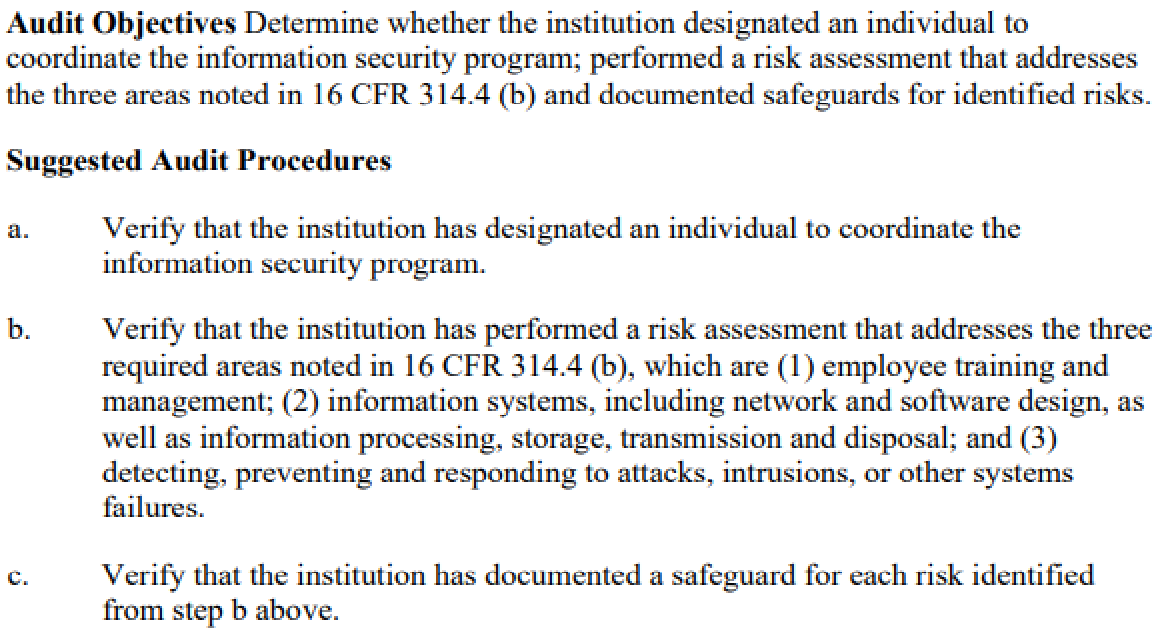
SFA - Title IV Programs

Compliance Requirements The Gramm-Leach-Bliley Act (Public Law 106-102) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data (16 CFR 314). The Federal Trade Commission considers Title IV-eligible institutions that participate in Title IV Educational Assistance Programs as "financial institutions" and subject to the Gramm-Leach-Bliley Act because they appear to be significantly engaged in wiring funds to consumers (16 CFR 313.3(k)(2)(vi). Under an institution's Program Participation Agreement with the ED and the Gramm-Leach-Bliley Act, institutions must protect student financial aid information, with particular attention to information provided to institutions by ED or otherwise obtained in support of the administration of the federal student financial aid programs (16 CFR 314.3; HEA 483(a)(3)(E) and HEA 485B(d)(2)). ED provides additional information about cybersecurity requirements at https://ifap.ed.gov/fsa-cybersecurity-compliance.

https://www.whitehouse.gov/wp-content/uploads/2020/08/2020-Compliance-Supplement_FINAL_08.06.20.pdf

Steps in Preparing for 2021 Audit

- **Review prior compliance supplement**



Audit Objectives Determine whether the institution designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.

Suggested Audit Procedures

a. Verify that the institution has designated an individual to coordinate the information security program.

b. Verify that the institution has performed a risk assessment that addresses the three required areas noted in 16 CFR 314.4 (b), which are (1) employee training and management; (2) information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) detecting, preventing and responding to attacks, intrusions, or other systems failures.

c. Verify that the institution has documented a safeguard for each risk identified from step b above.

https://www.whitehouse.gov/wp-content/uploads/2020/08/2020-Compliance-Supplement_FINAL_08.06.20.pdf

Discussion: Remote Workforce and the Impact on Higher Education Institutions

SolarWinds Update and Potential Impact on Higher Education

Summary and Current State of SolarWinds

1. SolarWinds (SW) development/update process is compromised
   - Malware added to plug in component
2. Customers download and install SW update with back door malware
   - Legitimate appearing malware installed
3. Sophisticated malware “scans” location
   - Gathers information (“where am I”)
   - Attacks/disables security tools
4. Malware “phones home”
   - Connects to Command and Control Server (C2)
   - Provides recon information and accepts instructions
5. Some organizations are subject to additional attack activity
   - Lateral movement/pivoting
   - Privilege escalation
   - Creation of additional/secondary persistence mechanisms
6. Objectives?
   - Gather and steal information?
   - Launch point for attack into other trusted systems?
     - ➢ Office 365?
     - ➢ Other trusted applications/systems?
     - ➢ Other trusted organizations?

Summary and Current State of SolarWinds

A. Sunspot
   - Malware designed to compromise software development process (at SolarWinds)

B. Sunburst
   - Backdoor inserted by Sunspot

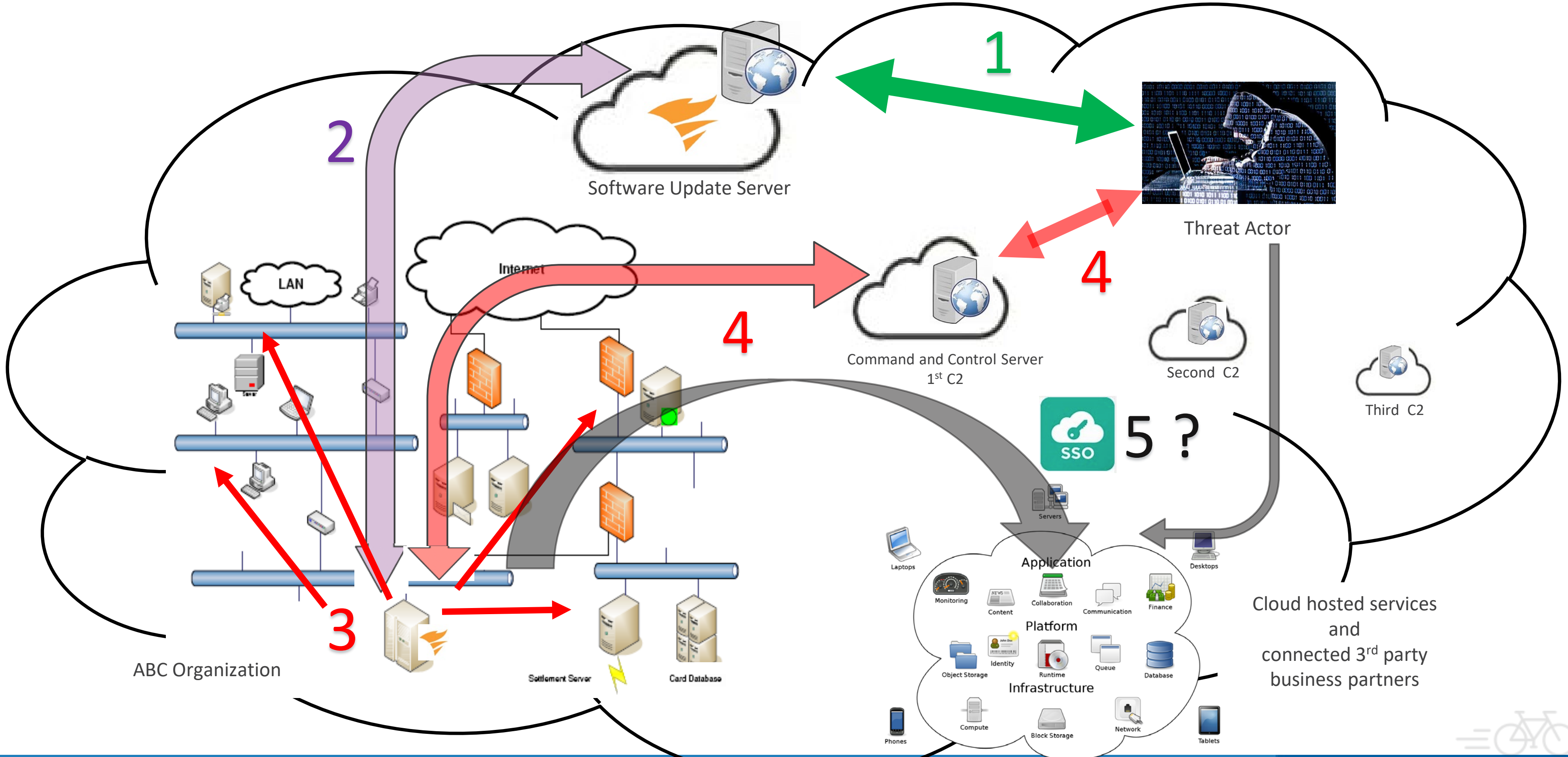
C. Teardrop
   - Installed via Sunburst backdoor for additional follow on / focused attacks

D. Raindrop
   - Loader that delivers Cobalt Strike
   - NOT delivered by Sunburst
   - Usually delivered/used later in compromise and privilege escalation process

E. Some organizations are subject to additional attack activity
   - Lateral movement/pivoting
   - Privilege escalation
   - Creation of additional/secondary persistence mechanisms

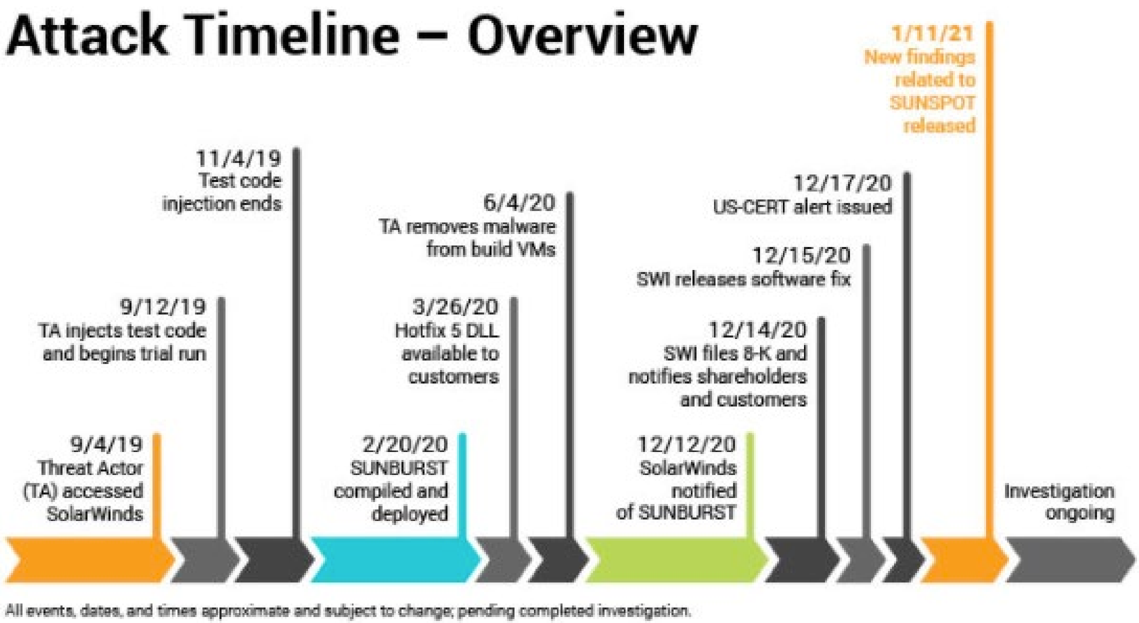
F. Objectives?
   - Gather and steal information?
   - Launch point for attack into other trusted systems?
     - ➢ Office 365?
     - ➢ Other trusted applications/systems?
     - ➢ Other trusted organizations?
     - ➢ "Golden SAML"

Picture in Your Minds Eye – SolarWinds Orion Compromise



Timeline of Events

Krebs On Security



Attack Timeline – Overview

9/4/19 Threat Actor (TA) accessed SolarWinds

9/12/19 TA injects test code and begins trial run

11/4/19 Test code injection ends

2/20/20 SUNBURST compiled and deployed

3/26/20 Hotfix 5 DLL available to customers

6/4/20 TA removes malware from build VMs

12/12/20 SolarWinds notified of SUNBURST

12/14/20 SWI files 8-K and notifies shareholders and customers

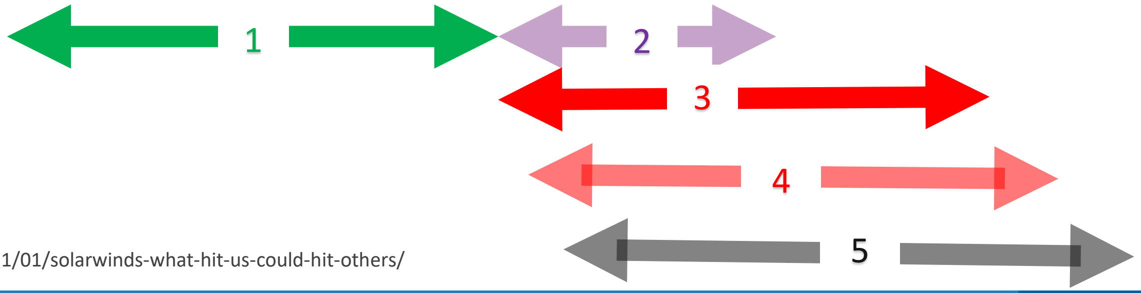
12/15/20 SWI releases software fix

12/17/20 US-CERT alert issued

1/11/21 New findings related to SUNSPOT released

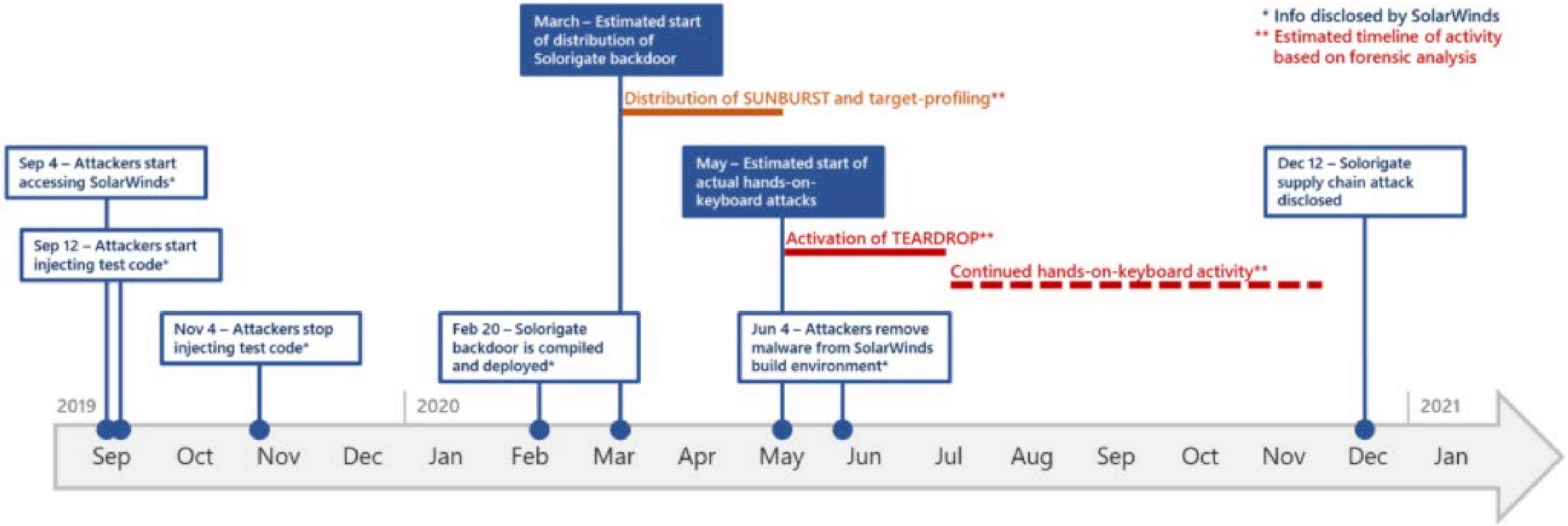
Investigation ongoing

All events, dates, and times approximate and subject to change; pending completed investigation.



https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/

Microsoft Timeline



* Info disclosed by SolarWinds

** Estimated timeline of activity based on forensic analysis

Sep 4 – Attackers start accessing SolarWinds*

Sep 12 – Attackers start injecting test code*

Nov 4 – Attackers stop injecting test code*

Feb 20 – Solorigate backdoor is compiled and deployed*

March – Estimated start of distribution of Solorigate backdoor

Distribution of SUNBURST and target-profiling**

May – Estimated start of actual hands-on-keyboard attacks

Activation of TEARDROP**

Continued hands-on-keyboard activity**

Jun 4 – Attackers remove malware from SolarWinds build environment*

Dec 12 – Solorigate supply chain attack disclosed

Figure 1. Timeline of the protracted Solorigate attack

https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Take-Aways

1. Do we use SolarWinds Orion?
   - If ***NO*** → Go to 6
   - If YES → What version?
2. Is our version the affected version (see SW advisory)?
   - If ***NO*** → Go to 6
   - If YES → Continue
3. Have we created a timeline of potential exposure?
4. What logs do we have and how far back in time do they go?
5. What Indicators of Compromise (IOC's) have we searched for?
   - What resources/references have we used to identify known and potential IOC's?
   - Use 3 and 4 to search for IOC's
6. Do we have any third-party service providers with trusted access?
   - Who has remote access into our environment?
   - Who do we push our data out to?
   - Are there any persistent open connections to or from third parties?
7. Repeat 1-5 for those identified in 6

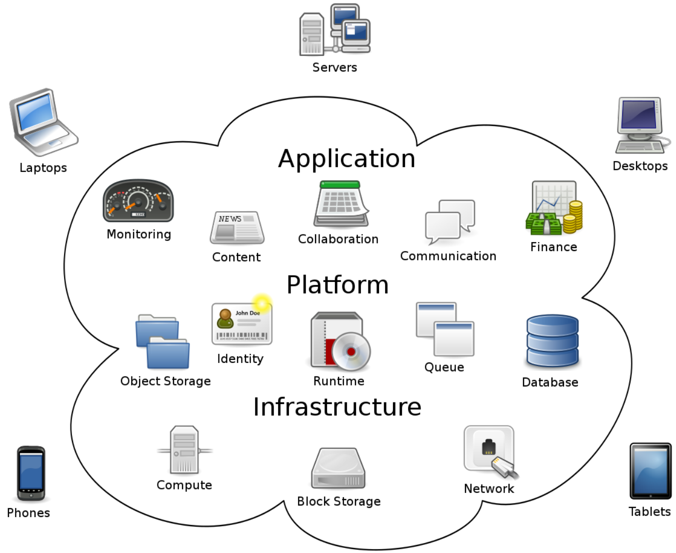
Take-Aways

8. “Know What Normal Looks like”
   - Easy to say… Challenging to execute
   - Server communication to the outside
9. Logs: DNS, Firewalls/Proxies, Windows…
   - Capture information about a newly-seen, unfamiliar domain in network traffic.
   - Leverage internal data sources and continuous DNS monitoring. Own-network defense is best augmented through visibility of own-network activity and traffic
   - Monitoring for new, unique, or abnormal network connections can identify C2 communication schema.
   - Proper asset classification which identifies specific hosts or host-type (e.g., “server” instead of “end-user client”) can further differentiate communication to identify items of concern.
   - Similar classification can also work to identify unusual authentication activity, where servers (such as a SolarWinds Orion device) initiate logons to other clients instead of the reverse.

https://www.domaintools.com/resources/blog/continuous-eruption-further-analysis-of-the-solarwinds-supply-incident

Take-Aways

9. Threat Hunting in Cloud Infrastructure
   - Mandiant Azure AD Investigator
   - CISA Sparrow
   - MS Azure Security Compass
10. Inhouse changes
    - Privileged accounts and service accounts
11. New information is being released every 2-3 days…



References and Resources

Microsoft Advisory

- https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
- https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
- https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/
- https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

FireEye Advisory

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

SolarWinds Advisory

- https://www.solarwinds.com/securityadvisory

NSA Advisory

- https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF

KrebsOnSecurity

- https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/
- https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/
- https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/

References and Resources

KrebsOnSecurity

- https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/
- https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/
- https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/

Domain Tools

- https://www.domaintools.com/resources/blog/continuous-eruption-further-analysis-of-the-solarwinds-supply-incident

Crowd Strike

- https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

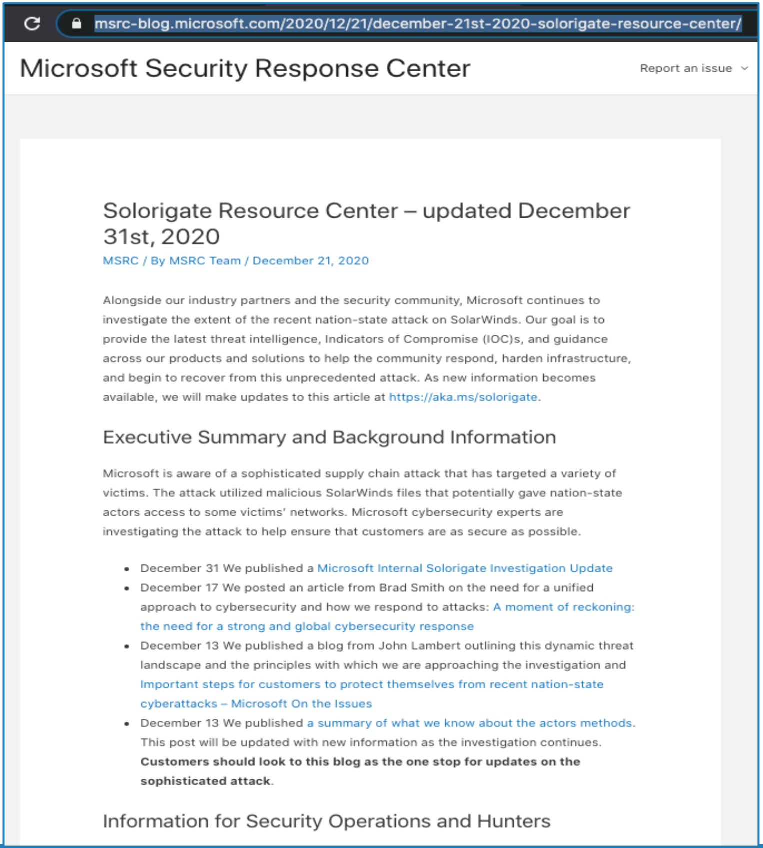
Symantec

- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

CLA Blog

- https://blogs.claconnect.com/Cybersecurity/solarwinds-orion-vulnerability/

References and Resources



msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/

Microsoft Security Response Center

Report an issue

Solorigate Resource Center – updated December 31st, 2020

MSRC / By MSRC Team / December 21, 2020

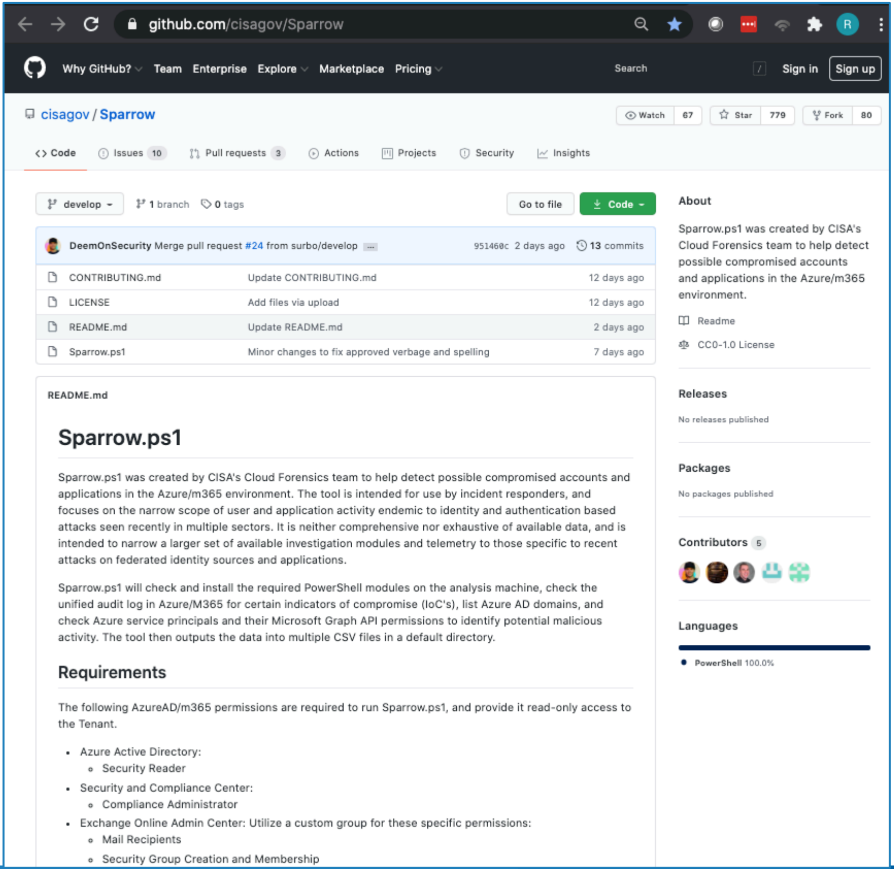
Alongside our industry partners and the security community, Microsoft continues to investigate the extent of the recent nation-state attack on SolarWinds. Our goal is to provide the latest threat intelligence, Indicators of Compromise (IOC)s, and guidance across our products and solutions to help the community respond, harden infrastructure, and begin to recover from this unprecedented attack. As new information becomes available, we will make updates to this article at https://aka.ms/solorigate.

Executive Summary and Background Information

Microsoft is aware of a sophisticated supply chain attack that has targeted a variety of victims. The attack utilized malicious SolarWinds files that potentially gave nation-state actors access to some victims' networks. Microsoft cybersecurity experts are investigating the attack to help ensure that customers are as secure as possible.

- December 31 We published a Microsoft Internal Solorigate Investigation Update
- December 17 We posted an article from Brad Smith on the need for a unified approach to cybersecurity and how we respond to attacks: A moment of reckoning: the need for a strong and global cybersecurity response
- December 13 We published a blog from John Lambert outlining this dynamic threat landscape and the principles with which we are approaching the investigation and Important steps for customers to protect themselves from recent nation-state cyberattacks – Microsoft On the Issues
- December 13 We published a summary of what we know about the actors methods. This post will be updated with new information as the investigation continues. **Customers should look to this blog as the one stop for updates on the sophisticated attack.**

Information for Security Operations and Hunters



github.com/cisagov/Sparrow

cisagov / Sparrow

DeemOnSecurity Merge pull request #24 from surbo/develop … 951460c 2 days ago 13 commits

CONTRIBUTING.md	Update CONTRIBUTING.md	12 days ago
LICENSE	Add files via upload	12 days ago
README.md	Update README.md	2 days ago
Sparrow.ps1	Minor changes to fix approved verbage and spelling	7 days ago

README.md

Sparrow.ps1

Sparrow.ps1 was created by CISA's Cloud Forensics team to help detect possible compromised accounts and applications in the Azure/m365 environment. The tool is intended for use by incident responders, and focuses on the narrow scope of user and application activity endemic to identity and authentication based attacks seen recently in multiple sectors. It is neither comprehensive nor exhaustive of available data, and is intended to narrow a larger set of available investigation modules and telemetry to those specific to recent attacks on federated identity sources and applications.

Sparrow.ps1 will check and install the required PowerShell modules on the analysis machine, check the unified audit log in Azure/M365 for certain indicators of compromise (IoC's), list Azure AD domains, and check Azure service principals and their Microsoft Graph API permissions to identify potential malicious activity. The tool then outputs the data into multiple CSV files in a default directory.

Requirements

The following AzureAD/m365 permissions are required to run Sparrow.ps1, and provide it read-only access to the Tenant.

- Azure Active Directory:
  - Security Reader
- Security and Compliance Center:
  - Compliance Administrator
- Exchange Online Admin Center: Utilize a custom group for these specific permissions:
  - Mail Recipients
  - Security Group Creation and Membership

About

Sparrow.ps1 was created by CISA's Cloud Forensics team to help detect possible compromised accounts and applications in the Azure/m365 environment.

Readme

CC0-1.0 License

Releases

No releases published

Packages

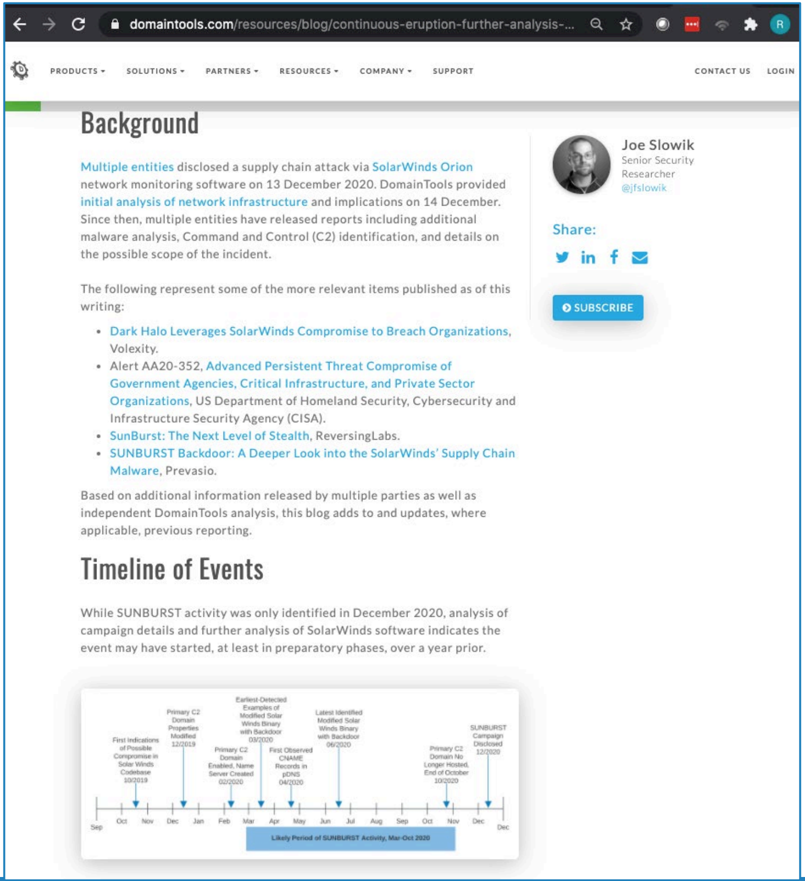
No packages published

Contributors 5

Languages

● PowerShell 100.0%

References and Resources



Background

Multiple entities disclosed a supply chain attack via SolarWinds Orion network monitoring software on 13 December 2020. DomainTools provided initial analysis of network infrastructure and implications on 14 December. Since then, multiple entities have released reports including additional malware analysis, Command and Control (C2) identification, and details on the possible scope of the incident.

The following represent some of the more relevant items published as of this writing:

- Dark Halo Leverages SolarWinds Compromise to Breach Organizations, Volexity.
- Alert AA20-352, Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA).
- SunBurst: The Next Level of Stealth, ReversingLabs.
- SUNBURST Backdoor: A Deeper Look into the SolarWinds' Supply Chain Malware, Prevasio.

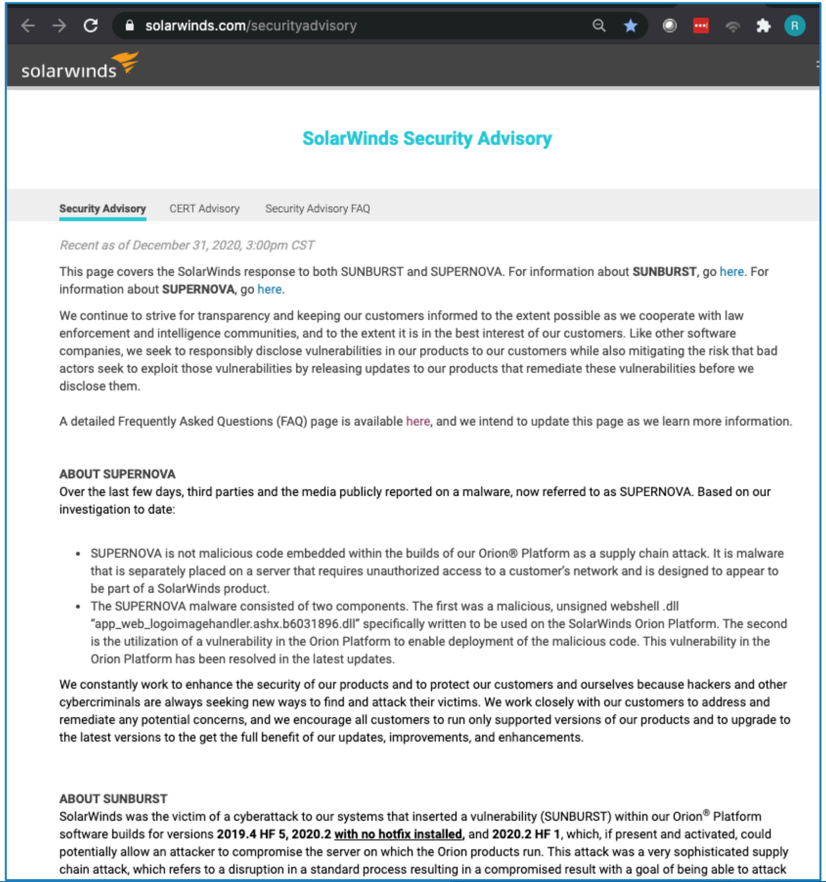
Based on additional information released by multiple parties as well as independent DomainTools analysis, this blog adds to and updates, where applicable, previous reporting.

Joe Slowik
Senior Security Researcher
@jfslowik

Timeline of Events

While SUNBURST activity was only identified in December 2020, analysis of campaign details and further analysis of SolarWinds software indicates the event may have started, at least in preparatory phases, over a year prior.

First Indications of Possible Compromise in Solar Winds Codebase 10/2019
Primary C2 Domain Properties Modified 12/2019
Primary C2 Domain Enabled, Name Server Created 02/2020
Earliest-Detected Examples of Modified Solar Winds Binary with Backdoor 03/2020
First Observed CNAME Records in pDNS 04/2020
Latest Identified Modified Solar Winds Binary with Backdoor 06/2020
Primary C2 Domain No Longer Hosted, End of October 10/2020
SUNBURST Campaign Disclosed 12/2020
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Dec
Likely Period of SUNBURST Activity, Mar-Oct 2020



solarwinds.com/securityadvisory
solarwinds

SolarWinds Security Advisory

Security Advisory
CERT Advisory
Security Advisory FAQ

Recent as of December 31, 2020, 3:00pm CST

This page covers the SolarWinds response to both SUNBURST and SUPERNOVA. For information about **SUNBURST**, go here. For information about **SUPERNOVA**, go here.

We continue to strive for transparency and keeping our customers informed to the extent possible as we cooperate with law enforcement and intelligence communities, and to the extent it is in the best interest of our customers. Like other software companies, we seek to responsibly disclose vulnerabilities in our products to our customers while also mitigating the risk that bad actors seek to exploit those vulnerabilities by releasing updates to our products that remediate these vulnerabilities before we disclose them.

A detailed Frequently Asked Questions (FAQ) page is available here, and we intend to update this page as we learn more information.

ABOUT SUPERNOVA
Over the last few days, third parties and the media publicly reported on a malware, now referred to as SUPERNOVA. Based on our investigation to date:

- SUPERNOVA is not malicious code embedded within the builds of our Orion® Platform as a supply chain attack. It is malware that is separately placed on a server that requires unauthorized access to a customer's network and is designed to appear to be part of a SolarWinds product.
- The SUPERNOVA malware consisted of two components. The first was a malicious, unsigned webshell .dll "app_web_logoimagehandler.ashx.b6031896.dll" specifically written to be used on the SolarWinds Orion Platform. The second is the utilization of a vulnerability in the Orion Platform to enable deployment of the malicious code. This vulnerability in the Orion Platform has been resolved in the latest updates.

We constantly work to enhance the security of our products and to protect our customers and ourselves because hackers and other cybercriminals are always seeking new ways to find and attack their victims. We work closely with our customers to address and remediate any potential concerns, and we encourage all customers to run only supported versions of our products and to upgrade to the latest versions to the get the full benefit of our updates, improvements, and enhancements.

ABOUT SUNBURST
SolarWinds was the victim of a cyberattack to our systems that inserted a vulnerability (SUNBURST) within our Orion® Platform software builds for versions **2019.4 HF 5**, **2020.2** **with no hotfix installed**, and **2020.2 HF 1**, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run. This attack was a very sophisticated supply chain attack, which refers to a disruption in a standard process resulting in a compromised result with a goal of being able to attack

Thank you!

Randy Romes
CISSP, CRISC, CISA, MCP, PCI-QSA
Principal – Cyber Security Team
Direct: 612-397-3114
Randy.Romes@claconnect.com

Kadian Douglas, CISA, CPA
Principal
Direct: 813-384-2735
Kadian.Douglas@claconnect.com

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING