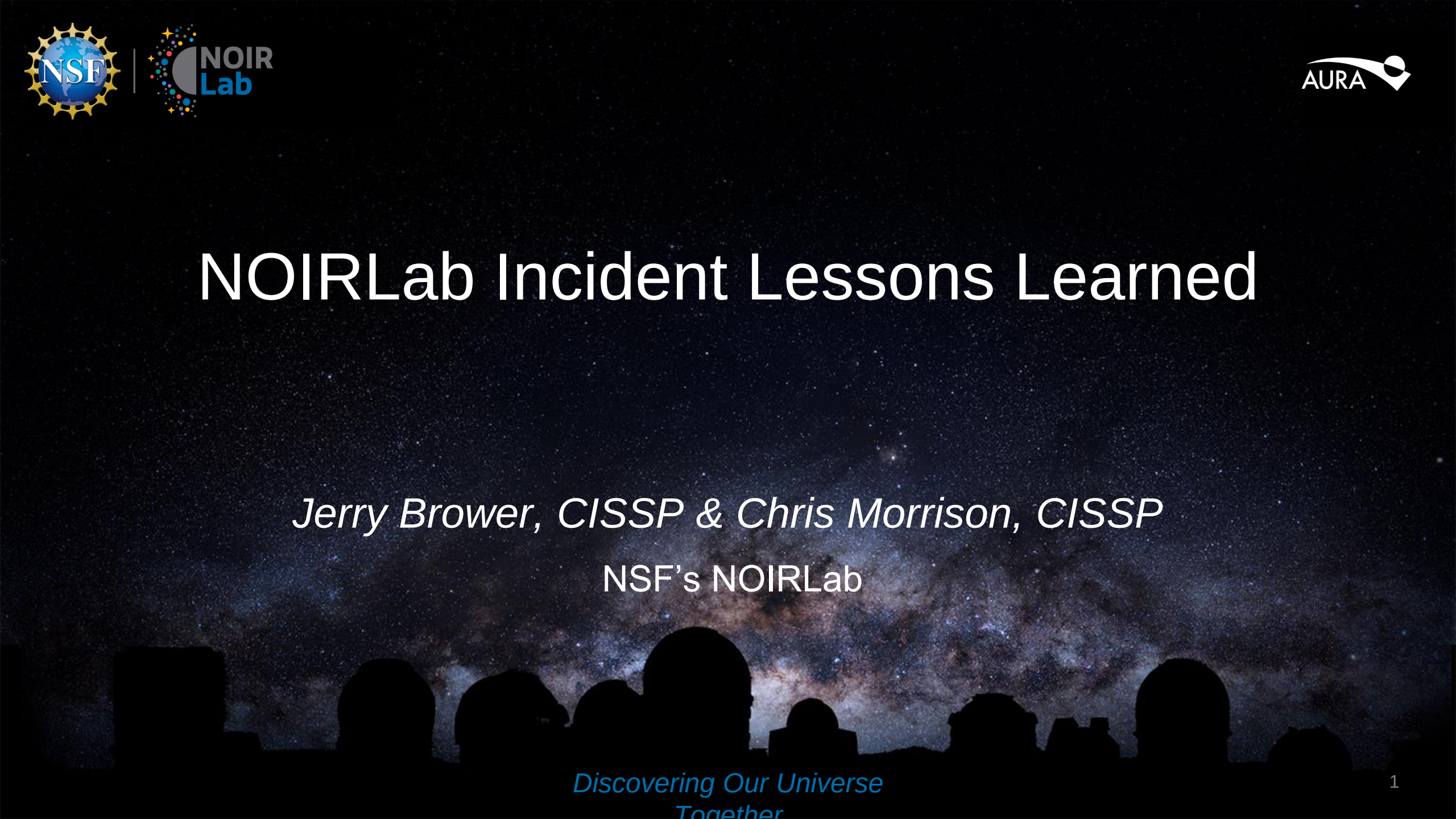
NOIRLab Incident Lessons Learned

Jerry Brower, CISSP & Chris Morrison, CISSP

NSF's NOIRLab



Discovering Our Universe Together

Overview

- Incident Summary
- Incident Response & Communications
- Infrastructure Enhancements
- A look at the Impact of the incident and recovery
- Key Takeaways
- Brief overview of where we are now

Incident Summary

- NOIRLab's Systems were compromised on August 1
- The incident was detected in real time and interrupted within 40 minutes
- Cybersecurity Incident Response Plan was activated
- Professionals in cybersecurity brought in to assist with response & forensics

Incident Summary

- Operations at Gemini North, Gemini South and most tenants on Cerro Tololo and Cerro Pachon suspended for 60 days
- Cloud-based services, such as email and Zoom were only briefly interrupted, due to SSO service availability
- Science operations returned to **new** normal

Incident Summary

- Protecting Critical Infrastructure was the focus of initial activities
  - Network and infrastructure are now hardened
    - Zero-Trust, Highly segmented & Isolated
      - *More details later*
- Followed by getting staff connected to internal networks
- Finally, establishing external traffic flows

Incident Response

Cybersecurity Incident Response Plan is Critical

Detection & Immediate Response

Engage Outside Experts

- Legal
- IR Vendor
- **Communications**

Investigation & Remediation

- Prevent damage
- Install Forensics Agent

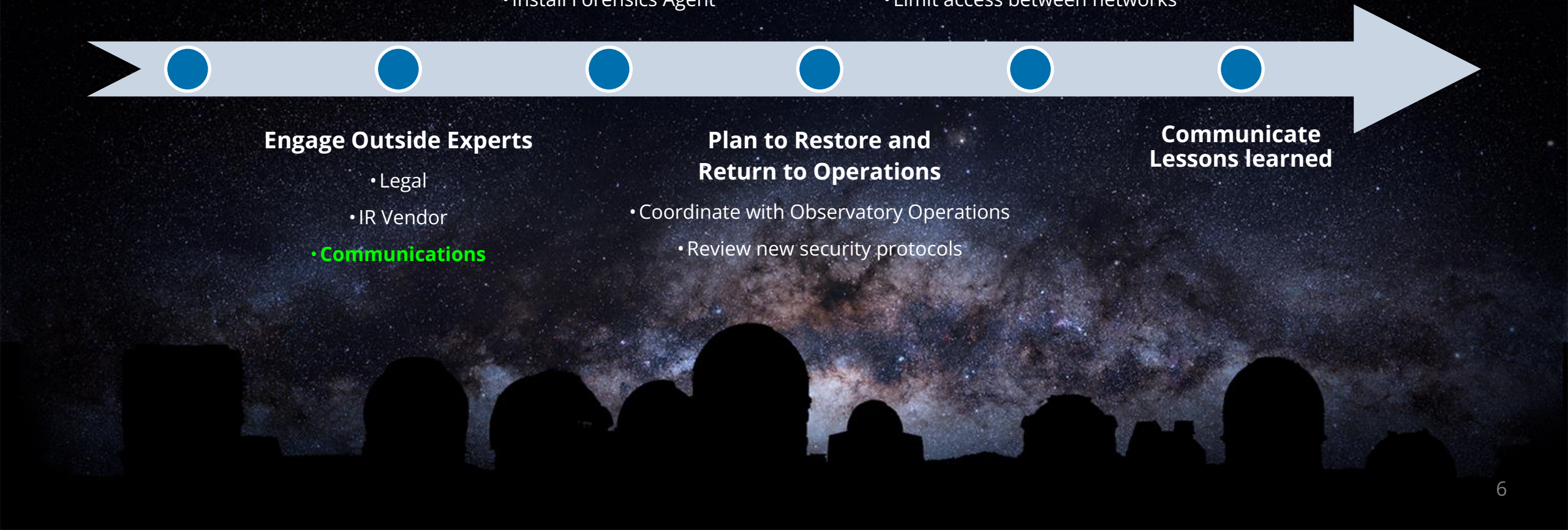
Plan to Restore and Return to Operations

- Coordinate with Observatory Operations
- Review new security protocols

Network/System Hardening

- Lock down critical infrastructure
- Limit access between networks

Communicate Lessons learned



Incident Response - Comms

- Regular communication with stakeholders - Limited
- NOIRLab ITOps continuous communication with
  - NOIRLab leadership
  - AURA HQ
  - NSF Leadership & NSF Cybersecurity Advisor
- Communications meetings with Public Relations advisors
- Communication with council present
- Limited communication with **NOIRLab staff**

Infrastructure Enhancements

- Systems and services locked down and hardened
- Secure administrator account management & Role-Based Access Control (RBAC)
- Privileged Access Management (PAM)
- End-Point Detection and Response (EDR)
- Multi-factor authentication (MFA) on all services, external **and internal**

Infrastructure Enhancements

- Network segmentation & Isolation
  - Controlled access management between network segments
- Tools and service to provide access to critical infrastructure and control access to network segments
- Restricted outbound traffic flow
- Limited outward-facing services - stop and question each process - **everywhere**!

Infrastructure Enhancements

- Recovering Remote Access
  - Remote access solutions for staff to **restricted** resources
  - Remote access for external collaborators to **internal** resources
  - Remote access for vendors to **do specific tasks** only
- Outside of the box solutions to minimize risk
- All remote access must be justified and approved

Incident Impact

Personal

Organizational (Staff, Workflows, Projects …)

SysAdmin Overhead

Operations

Enhancement Implementation Workload

Collaborators

Key Takeaways

- Have an incident response plan, it will remove uncertainties
- Protect Critical Infrastructure; this should be the focus of activities
- Implement layered security to access internal networks (zero-trust model) - as a must
- Have a look at the NSF Trusted CI Framework
  - **Focus on Transformative Twelve from Craig's talk yesterday**
- Have a Cybersecurity Strategic Plan and implement it!

Where are we now?

- Internal network access modified to layered security (zero-trust model)
- We have implemented around **75%** of all access requests, after **8 months**
- Cybersecurity Strategic Plan is being rewritten
- We are reviewing our communication plans:
  - Internal staff
  - External Collaborators
  - Stakeholders & neighbor organizations


Thank you,
Sap’e,
Mahalo,
Muchas Gracias!